UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PROPUESTA DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA NUBE BASADOS EN NIST 800-53 E ISO-27000
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autora:
Ing. Evelin Maritza Gavilanes Quiroga
Tutor:
MSc. Ing. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA NUBE BASADOS EN NIST 800-53 E ISO-27000.

Elaborado por: Evelin Maritza Gavilanes Quiroga, de C.I: 1720142445, estudiante de la Maestría: Seguridad Informática, de la UNIVERSIDAD TECNOLÓGICA ISRAEL, como parte de los requisitos sustanciales con fines de obtener el Título de Magister en Seguridad Informática, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

_____

Firma

ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Evelin Maritza Gavilanes Quiroga con C.I: 1720142445, autora del proyecto de titulación denominado: PROPUESTA DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA NUBE BASADOS EN NIST 800-53 E ISO-27000. Previo a la obtención del título de Magister en Seguridad Informática.

Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.

Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
EVELIN MARITZA
GAVILANES QUIROGA

Firma

ORCID: 0000-0001-6990-9050

Tabla de contenidos

Índice de tablas

Índice de Figuras

INFORMACIÓN GENERAL

Después de la pandemia las empresas ven en los servicios de nube una opción para innovar y desarrollar soluciones tecnológicas más eficientes.

Contextualización del tema

Según Vera-Cruz (2021) en su artículo «Empresas en la nube: Oportunidades y riesgos que se deben considerar», de acuerdo con un estudio realizado por Accenture, el 81% de las empresas ubicadas en Latinoamérica adoptaron los servicios de nube de manera moderada o alta durante la pandemia. A nivel mundial, el 77% de las organizaciones afirmó tener al menos una aplicación en la nube. Según los resultados de esta investigación, el 94% de las empresas latinoamericanas consideran que la nube es una herramienta esencial para alcanzar sus objetivos de sustentabilidad, mientras que un 89% la ve como una forma de mitigar la incertidumbre y disminuir los riesgos del negocio, especialmente en tiempos de crisis.

El creciente uso de servicios en la nube en almacenamiento y procesamiento de datos de manera remota presenta un nuevo desafío tanto para las empresas proveedoras de estos servicios como para los usuarios; ya que según «Kaspersky» (2023), en los artículos «¿Qué es la seguridad en la nube?» y «Problemas y riesgos de la seguridad en la nube», los recursos almacenados y procesados en entornos de nube, no implica que esté libre de malware, inclusive existen códigos maliciosos diseñados para atacar específicamente a plataformas virtuales; además también es importante asegurarse de que las aplicaciones implementadas estén libres de vulnerabilidades o errores que puedan ser explotados por los ciberdelincuentes que buscan robar la información.

Otro de los principales desafíos es garantizar que solo el personal autorizado tenga acceso a los datos y sistemas alojados en la nube, para lograr esto, es esencial llevar a cabo una gestión adecuada de identidades y accesos, esto implica la necesidad de establecer políticas sólidas de autenticación y autorización en los servicios en la nube, junto con la implementación de medidas de seguridad adicionales, como el cifrado de datos y el monitoreo de accesos, así también contar con regulaciones y estándares de cumplimiento que puedan aplicarse a la información almacenada en la nube. Estas acciones permiten a las organizaciones asegurar la privacidad, integridad y disponibilidad de la información almacenada y procesada en la nube.

Igualmente es importante que los proveedores de servicios de nube implementen medidas de seguridad robustas en sus centros de datos para protegerse contra posibles ataques maliciosos, como ataques de denegación de servicio (DDoS) o infiltraciones de malware.

Según «Evaluando Cloud» (2018), en lo que corresponde a la seguridad de los servicios en la nube, tanto Microsoft y Google, enfatizan en que se trata de una responsabilidad compartida, el hecho de que la información no se encuentre en la infraestructura de cada organización no significa que esta responsabilidad recaiga únicamente en el proveedor del servicio, por lo que es importante que tanto el proveedor de servicios como el usuario cuenten con los métodos de seguridad y recuperación adecuados.

Por lo expuesto, es necesario aplicar medidas de seguridad adecuadas, la adopción de buenas prácticas y trabajar de manera sincronizada entre proveedores de servicios en la nube y usuarios, esto contribuira a reducir los riesgos asociados con servicios de nube y asegurar la seguridad de los datos. Todas estas consideraciones garantizan un ambiente seguro y confiable para los proveedores de servicios de nube y usuarios.

Problema de investigación

Según Vera-Cruz (2021), con las nuevas tecnologías como la inteligencia artificial (IA), Machine Learning (ML), la automatización, entre otras, son tecnologías que requieren procesar grandes capacidades de información, lo que conlleva problemas inevitables de latencia, ancho de banda y seguridad, siendo la seguridad un reto para muchas empresas tanto proveedoras como consumidoras de los servicios de nube; a pesar de que muchas de estas empresas adopten medidas de seguridad para proteger sus sistemas, en muchos casos la falta de conocimiento y comprensión en torno a la seguridad informática puede ocasionar errores en las configuraciones dejando vulnerables sus sistemas, por lo que es importante contar con controles que podrían ser considerados por las empresas que optan por migrar sus servicios a la nube como una estrategia en la transformación digital, que les permita mitigar los riesgos y asegurar la data de las amenazas a las que actualmente se enfrentan.

¿Con el modelo del Marco de Ciberseguridad de NIST, se puede proteger los sistemas en nube?

Objetivo general

Proponer un grupo de controles basados en la comparativa del NIST 800-53, la familia de la ISO-27000 y las mejores prácticas empleadas en proveedores de servicios nube.

Objetivos específicos

- Realizar una revisión del estado del arte que identifique buenas prácticas en seguridad en la nube.
- Comparar marcos y estándares de referencia que proponen controles para tecnología nube.
- Desarrollar una propuesta basada en las mejores prácticas para seguridad en la nube.

Vinculación con la sociedad y beneficiarios directos.

Este proyecto plantea desarrollar una propuesta basado en el análisis comparativo de marcos de referencia que propone controles para tecnología nube, así también contar con un documento que abarque los aspectos más relevantes referentes a los riesgos que se tiene en la nube.

Se encuentra asociado con el “Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación” de los Objetivos de Desarrollo Sostenible, ya que este objetivo promueve el acceso a internet a la población mundial, el establecimiento de estructuras robustas, el respaldo de la industrialización sostenible, la estimulación de la innovación y al crecimiento de la producción a través de diferentes tipos de empresas, esto implica que cada vez más personas y empresas en encuentren conectados al internet, por lo que es importante identificar los riesgos que esto conlleva y este estudio aportará con una propuesta basada en las mejores prácticas de esquemas para seguridad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Las organizaciones ven en los servicios en la nube una opción para innovar y desarrollar, sin embargo, es importante considerar los aspectos acerca de la seguridad de estos servicios.

1.1. Contextualización general del estado del arte

La adopción de la nube ha sido un impulso para la transformación digital para muchas empresas y entidades gubernamentales, sin embargo, de acuerdo Ramírez et al., (2017) este crecimiento y migración hacia la nube deriva en grandes retos para las empresas debido a que incorpora de manera nativa a la web, por lo que es importante tratar la seguridad en la nube de una manera estructurada.

La mayoría de proveedores de nube aseguran que la seguridad en última instancia es responsabilidad del cliente, mientras ellos solo se responsabilizan de sus centros de datos e infraestructura, lo que se denomina como entorno de seguridad compartido.

1.1.1. Computación en la Nube

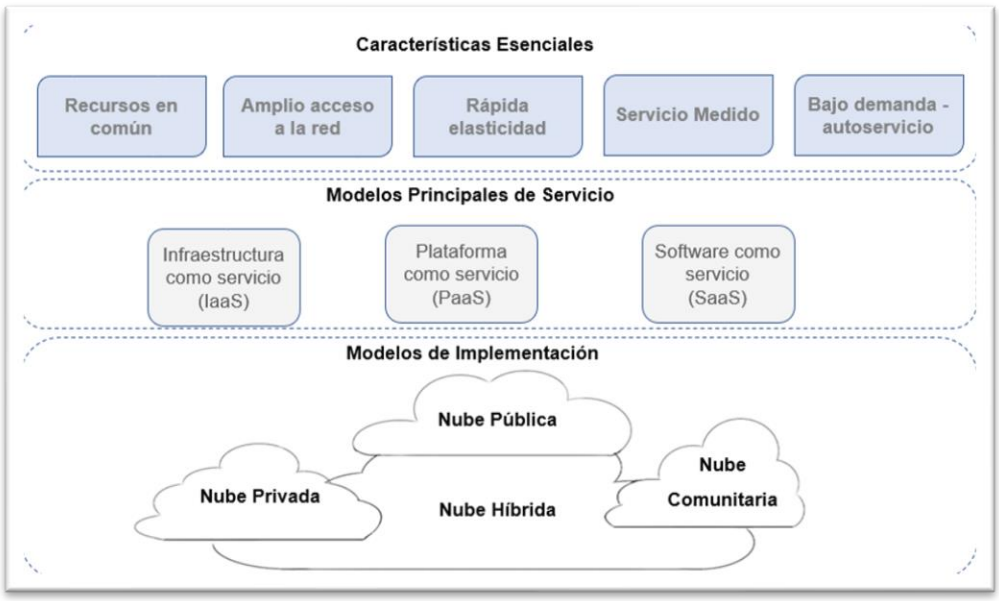
Según la definición establecida en el Instituto Nacional de Estándares y Tecnología (NIST) SP 800-145 (2011), la computación en la nube se refiere a un sistema que permite acceder a recursos informáticos, como almacenamiento, procesamiento, redes, aplicaciones y servicios, desde cualquier ubicación. Estos recursos son gestionables fácilmente y pueden configurarse y liberarse con mínima intervención administrativa o del proveedor.

La tecnología de nube está conformada por

- 5 Características Esenciales.
- 3 Modelos Principales de Servicio.
- 4 Modelos de Implementación.

Figura 1.

Características y Modelos de Nube



Nota: Por el autor, basado en varias fuentes.

a. Características esenciales

Recursos en común. - Los recursos informáticos se asocian para atender a múltiples usuarios mediante un modelo de múltiples inquilinos, asignando dinámicamente varios recursos físicos y virtuales según las necesidades de los usuarios. Existe una percepción de independencia de la ubicación, ya que el usuario normalmente no controla ni conoce la ubicación exacta del recurso proporcionado, sin embargo, se puede establecer de manera general la ubicación de los recursos como por ejemplo el país. Los recursos informáticos que se incluyen en este tipo de servicios son almacenamiento, procesamiento, redes, memoria y ancho de banda.

Amplio acceso a la red. - Los recursos se entrega por medio de la red, el acceso es por intermedio de mecanismos estándar que facilitan plataformas heterogéneas de clientes ligeros o pesados como tabletas, teléfonos móviles, computadoras portátiles y de escritorio.

Rápida elasticidad. - La capacidad se puede aprovisionar y liberar de manera flexible, en ciertos casos de manera automática para expandirse rápidamente según la demanda. Para los consumidores la capacidad disponible para el suministro suele parecer ilimitada ya que se puede configurar de manera indistinta del momento y cantidad.

Servicio Medido. - Hace referencia al servicio de nube donde se supervisa y optimiza de forma automática el consumo de los recursos de nube a través de capacidades de medición, generalmente sobre una base de pago por uso o tarifa por uso, para varios tipos de servicios, como son recursos de almacenamiento, memoria, procesamiento, infraestructura de red, ancho de banda y cuentas de usuario activas. Para garantizar transparencia en el consumo de recursos estos se pueden monitorear, supervisar y reportar.

Bajo demanda - autoservicio. - Los consumidores pueden configurar recursos informáticos de forma automática y unilateral según se requiera, con independencia de comunicación con cada proveedor de servicios.

b. Principales modelos de servicio

Software como servicio (SaaS). - En este modelo la administración y ubicación de las aplicaciones son realizadas por un proveedor de nube, es el responsable de gestionar versiones y actualizaciones. Los proveedores de nube permiten a los usuarios acceder a estos servicios desde una variedad de dispositivos, como computadoras, teléfonos inteligentes o tabletas.

Plataforma como servicio (PaaS). - Este modelo el usuario realiza la implementación de la infraestructura que construyen o adquieren en la nube, donde a menudo se combinan varias máquinas virtuales. Dichos servicios permiten a los desarrolladores crear múltiples aplicaciones con base en las herramientas proporcionadas por el proveedor de servicios.

Infraestructura como servicio (IaaS). - Para este modelo, los usuarios adquieren recursos informáticos básicos, como procesamiento, almacenamiento y redes, los consumidores tienen la libertad de desplegar cualquier tipo de software o aplicaciones propias de cada organización.

c. Modelos de implementación

Nube privada. - En este modelo la infraestructura está diseñada para ser dedicada a una organización, por lo general se aloja en el centro de datos propio de cada organización y puede ser propiedad de dicha organización, la administración de la infraestructura puede ser responsabilidad de la organización, por un tercero o por una combinación de ambos.

Nube comunitaria. - En este modelo, la infraestructura tecnológica está configurada para uso de una comunidad definida por organizaciones con un propósito común. Puede ser propiedad de una o más organizaciones comunitarias, terceros o una combinación de ellos, quienes son responsables de la gestión de la infraestructura, y puede estar alojada dentro o fuera de las instalaciones.

Nube pública. - Los recursos informáticos están disponibles para uso público. Puede ser propiedad de una organización comercial, académica, gubernamental o una combinación de estas; quienes son los encargados de operar y administrar la infraestructura. La infraestructura se localiza en las instalaciones de los proveedores de la nube.

Nube híbrida. – Está conformada por dos o más modelos de nube ya sean privada, comunitaria o pública, bajo una sola organización, pero vinculadas por tecnologías patentadas o estandarizadas que admiten la portabilidad de datos y aplicaciones.

1.1.2. Adopción de servicios en la Nube

En la actualidad la computación en la nube se ha convertido en un modelo de referencia para organizaciones que están en vías de transformación digital; según el ranking de Cloud Wars de «Acceleration Economy» (2023), los 10 proveedores de nube más influyentes del mundo son: Microsoft, Google Cloud, Amazon, Oracle, SAP, Salesforce, IBM, Workday, snowflake y ServiceNow.

a) Crecimiento de Nube

Según Muñoz (2021) actualmente existen tres grandes servicios en la nube, que son:

- SaaS - Software como servicio
- PaaS - Plataforma como servicio
- IaaS - Infraestructura como servicio

Así también, de acuerdo con la consultora global «Corporación Internacional de Datos» - IDC (2022), el mercado global de servicios de nube pública, en estos modelos, experimento un crecimiento del 29,0% al 2021.

Tabla 1.
Crecimiento de Servicios de Nube

Categoría de Implementación	Crecimiento al 2021
IaaS	35.6%
PaaS	39.1%
SaaS – Aplicaciones	23.5%
SaaS: Software de Infraestructura del Sistema	26.4%
Total	**29.0%**

Nota: Tomado de International Data Corporation (IDC)

1.1.3. Ventajas y Desafíos con la computación en la nube

La computación en la nube permite a las empresas acceder y almacenar su información a través de Internet, desde cualquier lugar y sin necesidad de administrar su infraestructura.

a) Ventajas

De acuerdo con Cisco (sf) los principales beneficios de esta tecnología son:

- Reducción de costos
- Facilidad de implementación
- Flexibilidad
- Escalabilidad
- Reasignación del personal
- Sostenibilidad

b) Desafíos

A pesar de los beneficios en términos de escalabilidad, flexibilidad y rentabilidad, existen desafíos y riesgos vinculados a la implementación de esta tecnología. Las empresas deben estar conscientes de los posibles desafíos y riesgos que podrían enfrentar.

De acuerdo con FORTINET (2022) los entornos de nube presentan varios desafíos de seguridad como son:

- Contar con los conocimientos adecuados para la implementación y administración de una solución completa.

- Garantizar la protección y privacidad de la data en los diferentes entornos de nube.
- Tener claridad sobre las diferentes soluciones de nube.
- Pérdida de visibilidad y control en los entornos de nube

Según el informe de «European Union Agency for Cybersecurity» ENISA, (2022) los riesgos más significativos identificados para entornos de nube se exponen en la tabla 2:

Tabla 2.
Riesgos en la Computación en la Nube

Riesgo	Descripción
Pérdida de Gobernanza	En la infraestructura de nube, el usuario de manera obligada cede el control al proveedor de nube, de una serie de aspectos que influyen en la seguridad.
Vinculación	No existen herramientas, métodos o formatos de datos estandarizados, ni interfaces de servicio que aseguren la transferencia fluida de servicios en la nube. Por esta razón, la migración de los servicios a la nube puede ser compleja.
Fallo de Aislamiento	La característica distintiva de la computación en la nube es su capacidad de ofrecer múltiples servicios y compartir recursos de manera eficiente. El error de los mecanismos que separan los recursos de cómputo, como el almacenamiento, la memoria, el enrutamiento, representan una vulnerabilidad que podría conllevar los denominados ataques «guest hopping», así también, se debe tener en cuenta los posibles ataques a los mecanismos de aislamiento de recursos como los hipervisores.
Riesgos de Cumplimiento	Inversión para la certificación de requisitos reglamentarios o normativos del sector, como por ejemplo PCI DSS.
Interfaz de Gestión	Las interfaces utilizadas para administrar los recursos de nube, por lo general son de acceso público a través de Internet, esto plantea un mayor riesgo, especialmente cuando se combina con el acceso remoto y las vulnerabilidades del navegador web.

Riesgo	Descripción
Protección de Datos	La computación en la nube plantea muchos riesgos de privacidad de datos tanto para los clientes como para los proveedores de servicios en la nube. Para los usuarios de estos servicios, verificar de manera efectiva las estrategias de administración de los datos puede ser una tarea compleja. Esto puede generar desafíos para garantizar que sus datos estén siendo manejados en concordancia con las regulaciones legales.
Supresión de Datos Insegura o Incompleta	Al igual que con la mayoría de los sistemas informáticos, solicitar la eliminación de un recurso en la nube en ocasiones estos datos no se eliminan de forma permanente. Eliminar datos correctamente o de manera oportuna también puede ser casi imposible.
Miembro Malicioso	Por lo general, no se generan de forma regular, sin embargo, el daño causado por miembros malintencionados suele ser mucho más dañino. Las arquitecturas en la nube demandan capacidades con perfiles de riesgo bien definidos.

Nota: Tomado de European Union Agency for Cybersecurity (ENISA)

En algunos casos, Phun (2022) analista senior de software de «IDC América Latina» expresa una tendencia a creer que los servidores locales brindan más confianza, por lo que; muchas veces se asume que toda la capa de seguridad está del lado del proveedor de servicios; este no es el caso, y las preocupaciones de seguridad siguen siendo comunes tanto para proveedores de servicio de nube como para usuarios finales.

La seguridad es un factor importante a considerar previo a la migración de servicios a la nube, así como los usuarios almacenan una gran cantidad de información en sus computadoras, al utilizar los servicios en la nube, estos datos se transfieren desde su computadora hacia un entorno de nube por lo que son susceptibles a riesgos tanto en tránsito como en procesamiento y almacenamiento en la nube, por lo tanto, se debe contar con medidas de seguridad efectivas para proteger estos datos.

1.1.4. Seguridad en la nube

Como se indica en «Fire Eye» (2021), en su artículo «Cyber Security Predictions», a medida que se expande la adopción de la nube, las

organizaciones deberán aumentar la visión de huella en la nube, identificar los activos críticos en la nube y las comunicaciones con los proveedores para administrar el riesgo.

Asi también indica que cerca del 95% de las empresas tienen algún tipo de presencia en la nube, aunque solo sea para funciones internas, así también muchas empresas aplazan la implementación de autenticación multifactor, a los sistemas heredados a medida que aceleraban su migración a las plataformas en la nube en los últimos años. La urgencia de los requisitos comerciales a menudo impulsa a las organizaciones a avanzar más rápido en los esfuerzos de adopción de tecnología sin contar con los controles de seguridad adecuados. Es por esto por lo que las organizaciones necesitan proteger los métodos de acceso a los datos, y eso significa centrarse en la gestión de acceso e identidad y revisar quién califica para el acceso privilegiado.

Muchas de las amenazas en la nube son las mismas que las que se encuentran en las instalaciones del cliente, por lo que, se estima que los ataques en la nube continúen ejecutándose a través de:

- Robo de credenciales, regularmente a través de phishing
- Explotación de configuraciones erróneas
- Hackeo de aplicaciones vulnerables

Cuando se trata de una tecnología relativamente nueva como la nube, existen amplias oportunidades de error, por lo que las organizaciones deben centrarse en la preparación y la gestión de activos. El seguimiento completo y preciso de los activos en la nube debería ser una prioridad.

De acuerdo con el informe de seguridad en la nube de Fortinet (2022), el mayor riesgo de seguridad que pone en riesgo la privacidad de los datos es la mala configuración de plataformas de nube, seguido por las interfaces de aplicación (APIs) no seguras, exfiltración de información confidencial y accesos no autorizados.

Así también según el estudio de Thales (2021) se destaca las principales tecnologías que utilizan las organizaciones para proteger sus datos en entornos de nube, como son el cifrado de datos, seguido de la gestión de claves y finalmente el Múltiple Factor de Autenticación (MFA), siendo necesario ejecutar estas tres tecnologías para salvaguardar los datos en la nube, sin dejar de lado la aplicación de controles a través de políticas de seguridad con las que deben contar las empresas.

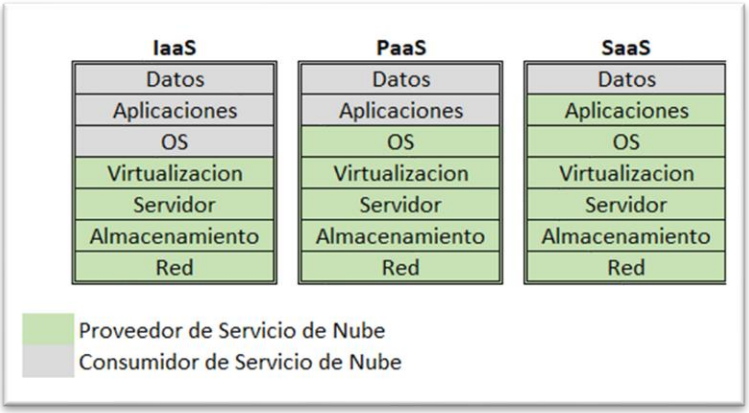
1.1.5. Responsabilidad de seguridad

Según Internal Revenue Service - IRS (2022), el modelo de servicio e implementación utilizado en un ambiente de nube determinará la responsabilidad de la aplicación de controles de seguridad entre los usuarios y los proveedores de servicios en la nube, para garantizar la protección de la información que se encuentra almacenada o es procesada.

La delimitación de la responsabilidad del control de seguridad depende en gran medida del modelo de servicio y los modelos de implementación. Por ejemplo, si se trata de una solución de correo electrónico (Servicio SaaS), la organización puede ser responsable de un pequeño subconjunto de responsabilidades de control de seguridad, incluidos los controles de acceso; en cambio, si se trata de implementación de sus propias aplicaciones en una solución PaaS o IaaS, tendrá una mayor responsabilidad de proteger la capa de la aplicación y, potencialmente la plataforma y el software intermedio (middleware).

De acuerdo Ramírez et al., (2017) a medida que se aumenta el nivel de abstracción de los servicios en nube, el cliente ejerce menor control sobre la infraestructura; de manera similar, cuanto más control tiene un cliente sobre la infraestructura proporcionada para el servicio, mayor capacidad tiene para aplicar medidas de seguridad y control
En la figura 2, se muestra un modelo de responsabilidad compartida en la nube entre el consumidor de servicios y el proveedor de nube para cada modelo revisado anteriormente.

Figura 2.
Modelo de Responsabilidad Compartida en la Nube



Nota: Por el autor, basado en varias referencias

1.2. Proceso investigativo metodológico

Este trabajo se basó en el método investigativo cualitativo con un enfoque exploratorio, basado en la revisión analítica de la literatura como son libros, informes, revistas científicas y sitios web, lo que permitió recopilar la información para describir el problema investigado.

En la investigación se analizó los controles de seguridad de las diferentes familias de NIST 800-53, y su aplicación en los proveedores de nube Amazon y Microsoft, que se encuentran dentro del top 10 en el ranking de «Cloud Wars» (2023), con esta base se planteó una propuesta de controles mínimos que deben ser implementados por las empresas proveedoras de servicios de nube; así también pueden ser una base para las organizaciones que planean certificarse en un sistema de seguridad de la información como ISO 27001.

1.3. Análisis de resultados

Las organizaciones proveedoras de servicios en la nube, que desean mejorar la gestión de la data y garantizar la seguridad de la información, disponen de varias opciones de normativas que pueden implementar; para este trabajo se realizó el análisis de una estrategia basada en 7 pasos de NIST-CSWP (2018) para la implementación del Marco Ciberseguridad del NIST, complementada con los controles de NIST 800-53 y su implementación en empresas proveedoras de servicios de nube.

A continuación, se muestra el estado inicial de los 298 controles de las veinte familias recomendados por la NIST 800-53, con un comparativo de los controles aplicados por Microsoft y Amazon (Anexos), donde se evidencia que las organizaciones pueden establecer los controles a utilizar dependiendo del más apropiado según sus necesidades.

Tabla 3.
Análisis Inicial

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
AC.	**Control de Acceso**						
AC-1	Política y procedimientos de control de acceso	√			√	√	√
AC-2	Administración de cuentas	√				√	√
AC-3	Control de acceso		√			√	√

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
AC-4	Control de flujo de información		√			√	√
AC-5	Separación de tareas	√				√	√
AC-6	Privilegios mínimos	√				√	√
AC-7	Intentos de inicio de sesión sin éxito		√			√	
AC-8	Notificación de uso del sistema			√		√	
AC-9	Notificación de inicio de sesión anterior		√				
AC-10	Control de sesión concurrente		√			√	
AC-11	Bloqueo		√			√	
AC-12	Terminación de la sesión		√			√	
AC-14	Acciones permitidas sin identificación o autenticación	√				√	
AC-16	Atributos de seguridad y privacidad	√				√	√
AC-17	Acceso remoto	√				√	√
AC-18	Acceso inalámbrico	√				√	√
AC-19	Control de acceso para dispositivos móviles	√				√	√
AC-20	Uso de sistemas externos	√				√	√
AC-21	El intercambio de información	√				√	√
AC-22	Contenido de acceso público	√				√	
AC-23	Protección de minería de datos	√					
AC-24	Decisiones de control de acceso	√					
AC-25	Monitor de referencia		√		√		
AT.	**Concientización y capacita**						
AT1	Política y procedimientos de conciencia y capacitación	√			√	√	
AT2	Entrenamiento y conciencia de alfabetización	√			√	√	√
AT3	Capacitación basada en roles	√			√	√	√
AT4	Registros de entrenamiento	√			√	√	
AT6	Comentarios de capacitación	√			√		
AU.	**Auditoría y Rendición de Cuentas**						
AU1	Política y procedimientos de auditoría y responsabilidad	√			√	√	
AU2	Registro de eventos	√				√	
AU3	Contenido de registros de auditoría		√			√	
AU4	Capacidad de almacenamiento de registros de auditoría			√		√	√
AU5	Respuesta a las fallas del proceso de registro de auditoría		√			√	
AU6	Revisión, análisis e informes de registros de auditoría	√			√	√	√
AU7	Reducción de registros de auditoría y generación de informes		√		√	√	√
AU8	Marcas de tiempo		√			√	
AU9	Protección de información de auditoría		√			√	
AU10	No repudio		√		√	√	
AU11	Retención de registros de auditoría	√			√	√	

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
AU12	Generación de registros de auditoría		√			√	√
AU13	Monitoreo de la divulgación de información	√			√		√
AU14	Auditoría		√		√		
AU16	Registro de auditorías de organización cruzada	√					
CA.	**Evaluación, Autorización y Seguimiento**						
CA1	Políticas y procedimientos de evaluación y autorización	√			√	√	
CA2	Evaluaciones de control	√			√	√	√
CA3	Intercambio de información	√			√	√	√
CA5	Plan de acción e hitos	√			√	√	
CA6	Autorización	√			√	√	
CA7	Monitoreo continuo	√			√	√	√
CA8	Pruebas de penetración	√			√	√	√
CA9	Conexiones internas del sistema	√			√	√	√
CM.	**Gestión de la configuración**						
CM1	Política y procedimientos de gestión de configuración	√			√	√	
CM2	Configuración de línea de base	√			√	√	√
CM3	Control de cambio de configuración	√			√	√	√
CM4	Análisis de impacto	√			√	√	√
CM5	Restricciones de acceso para el cambio	√				√	√
CM6	Ajustes de configuración			√		√	√
CM7	Menos funcionalidad			√		√	√
CM8	Inventario de componentes del sistema	√			√	√	√
CM9	Plan de gestión de configuración	√				√	√
CM10	Restricciones de uso de software	√				√	√
CM11	Software instalado por el usuario	√				√	√
CM12	Ubicación de información	√			√		
CM13	Mapeo de acción de datos	√					
CM14	Componentes firmados			√	√		
CP.	**Planificación de Contingencia**						
CP1	Política y procedimientos de planificación de contingencia	√			√	√	
CP2	Plan de contingencia	√				√	√
CP3	Capacitación de contingencia	√			√	√	√
CP4	Prueba del plan de contingencia	√			√	√	√
CP6	Sitio de almacenamiento alternativo	√				√	√
CP7	Sitio de procesamiento alternativo	√				√	
CP8	Servicios de telecomunicaciones	√				√	√
CP9	Copia de seguridad del sistema	√				√	√

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
CP10	Recuperación del sistema y reconstitución	√				√	√
CP11	Protocolos de comunicaciones alternativos	√					√
CP12	Modo seguro		√		√		
CP13	Mecanismos de seguridad alternativos			√			
IA.	**Identificación y Autenticación**						
IA1	Política y procedimientos de identificación y autenticación	√			√	√	
IA2	Identificación y autenticación (usuarios organizacionales)			√		√	
IA3	Identificación y autenticación del dispositivo		√			√	
IA4	Gestión de identificadores	√				√	
IA5	Gestión de autenticador			√		√	
IA6	Comentarios de autenticación		√			√	
IA7	Autenticación del módulo criptográfico		√			√	
IA8	Identificación y autenticación (usuarios no organizacionales)		√			√	
IA9	Identificación y autenticación del servicio			√			
IA10	Identificación y autenticación adaptativa	√					
IA11	Reautenticación			√			
IA12	Prueba de identidad	√					
IR.	**Respuesta Incidentes**						
IR1	Política y procedimientos de respuesta a incidentes	√			√	√	
IR2	Entrenamiento de respuesta a incidentes	√			√	√	
IR3	Prueba de respuesta a incidentes	√			√	√	√
IR4	Manejo de incidentes	√				√	√
IR5	Monitoreo de incidentes	√			√	√	√
IR6	Informe de incidentes	√				√	√
IR7	Asistencia de respuesta a incidentes	√				√	
IR8	Plan de respuesta a incidentes	√				√	√
IR9	Respuesta del derrame de información	√				√	
MA.	**Mantenimiento**						
MA1	Política y procedimientos de mantenimiento del sistema	√			√	√	
MA2	Mantenimiento controlado	√				√	√
MA3	Herramientas de mantenimiento	√				√	√
MA4	Mantenimiento no local	√				√	√
MA5	Personal de mantenimiento	√				√	√
MA6	Mantenimiento oportuno	√				√	
MA7	Mantenimiento de campo	√					
MP.	**Protección de Medios**						

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
MP1	Política y procedimientos de protección de medios	√			√	√	
MP2	Acceso a los medios	√				√	√
MP3	Marcado de medios	√				√	
MP4	Almacén de datos	√				√	√
MP5	Transporte de medios	√				√	√
MP6	Desinfeción de medios	√				√	√
MP7	Uso de los medios	√				√	√
MP8	Degradación de medios	√					
PE.	**Protección Física y Ambiental**						
PE1	Política y procedimientos de protección física y ambiental	√			√	√	
PE2	Autorizaciones de acceso físico	√				√	√
PE3	Control de acceso físico	√				√	√
PE4	Control de acceso para medio de transmisión	√				√	√
PE5	Control de acceso para dispositivos de salida	√				√	√
PE6	Monitoreo de acceso físico	√			√	√	√
PE8	Registros de acceso a los visitantes	√			√	√	
PE9	Equipo de energía y cableado	√				√	√
PE10	Cierre de emergencia	√				√	√
PE11	Potencia de emergencia	√				√	√
PE12	Iluminación de emergencia	√				√	√
PE13	Protección contra incendios	√				√	√
PE14	Controles ambientales	√				√	√
PE15	Protección de daños por agua	√				√	√
PE16	Entrega y eliminación	√				√	√
PE17	Sitio de trabajo alternativo	√				√	
PE18	Ubicación de los componentes del sistema	√				√	√
PE19	Fugas de información	√					√
PE20	Monitoreo y seguimiento de activos	√					√
PE21	Protección contra el pulso electromagnético	√					
PE22	Marcado de componentes	√					
PE23	Ubicación de las instalaciones	√					
PL.	**Planificación**						
PL1	Política y procedimientos de planificación	√			√	√	
PL2	Planes de seguridad y privacidad del sistema	√			√	√	√
PL4	Reglas de comportamiento	√			√	√	
PL7	Concepto de operaciones	√					
PL8	Arquitecturas de seguridad y privacidad	√			√	√	√

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
PL9	Gestión central	√			√		
PL10	Selección de línea de base	√					
PL11	Adaptación de línea de base	√					
PM.	**Programas de Gestión**						
PM1	Plan del programa de seguridad de la información	√					√
PM2	Rol de liderazgo del programa de seguridad de la información	√					
PM3	Seguridad de la información y recursos de privacidad	√					
PM4	Proceso de plan de acción e hitos	√					√
PM5	Inventario del sistema	√					
PM6	Medidas de rendimiento	√			√		√
PM7	Arquitectura empresarial	√					
PM8	Plan de infraestructura crítica	√					√
PM9	Estrategia de gestión de riesgos	√			√		√
PM10	Proceso de autorización	√			√		
PM11	Definición de la misión y el proceso de negocio	√					√
PM12	Programa de amenazas de información privilegiada	√			√		√
PM13	Fuerza laboral de seguridad y privacidad	√					√
PM14	Pruebas, capacitación y monitoreo	√			√		√
PM15	Grupos y asociaciones de seguridad y privacidad	√					√
PM16	Programa de conciencia de amenazas	√			√		√
PM17	Protección de información controlada no clasificada en sistemas externos	√			√		
PM18	Plan del programa de privacidad	√					
PM19	Rol de liderazgo del programa de privacidad	√					
PM20	Difusión de información del programa de privacidad	√			√		
PM21	Contabilidad de divulgaciones	√					
PM22	Gestión de calidad de información identificable personalmente	√			√		
PM23	Organismo de gobierno de datos	√			√		
PM24	Tablero de integridad de datos	√			√		
PM25	Minimización de información de identificación personal utilizada en pruebas, capacitación e investigación	√					
PM26	Gestión de reclamaciones	√					
PM27	Informes de privacidad	√					
PM28	Riesgo de enmarcado	√			√		
PM29	Roles de liderazgo del programa de gestión de riesgos	√					
PM30	Estrategia de gestión de riesgos de la cadena de suministro	√			√		
PM31	Estrategia de monitoreo continuo	√					

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
PM32	Propósito	√			√		
PS.	**Seguridad del personal**						
PS1	Política y procedimientos de seguridad de personal	√			√	√	
PS2	Designación de riesgos de posición	√				√	
PS3	Detección de personal	√				√	
PS4	Terminación del personal	√				√	
PS5	Transferencia de personal	√				√	
PS6	Acuerdos de acceso	√			√	√	
PS7	Seguridad de personal externo	√			√	√	√
PS8	Sanciones de personal	√				√	
PS9	Descripciones de posición	√					
PT	**Pii Procesamiento y Transparencia**						
PT1	Procesamiento de información de identificación personal y política y procedimientos de transparencia	√			√		
PT2	Autoridad para procesar información de identificación personal	√			√		
PT3	Propósitos de procesamiento de información identificable personalmente	√					
PT4	Consentir	√					
PT5	Aviso de Privacidad	√					
PT6	Aviso de Sistema de Registros	√					
PT7	Categorías específicas de información de identificación personal	√					
PT8	Requisitos de coincidencia de computadoras	√					
RA.	**Evaluación de Riesgos**						
RA1	Política y procedimientos de evaluación de riesgos	√			√	√	
RA2	Categorización de seguridad	√				√	√
RA3	Evaluación de riesgos	√			√	√	√
RA5	Monitoreo y escaneo de vulnerabilidad	√			√	√	√
RA6	Encuesta de contramedidas de vigilancia técnica	√			√		
RA7	Respuesta a los riesgos	√			√		
RA8	Evaluaciones de impacto de la privacidad	√			√		
RA9	Análisis de criticidad	√					
RA10	Caza de amenazas			√	√		
SA.	**Sistema y Adquisición de Servicios**						
SA1	Política y procedimientos de adquisición de sistemas y servicios	√			√	√	
SA2	Asignación de recursos	√			√	√	
SA3	Ciclo de vida de desarrollo de sistemas	√			√	√	√
SA4	Proceso de adquisición	√			√	√	√
SA5	Documentación del sistema	√			√	√	√

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
SA8	Principios de ingeniería de seguridad	√			√	√	√
SA9	Servicios de sistema externo	√			√	√	√
SA10	Gestión de configuración del desarrollador	√			√	√	√
SA11	Prueba y evaluación del desarrollador	√			√	√	√
SA15	Proceso de desarrollo, estándares y herramientas	√			√	√	√
SA16	Capacitación proporcionada por el desarrollador	√			√	√	
SA17	Seguridad de desarrollador y arquitectura y diseño de privacidad	√			√	√	√
SA20	Desarrollo personalizado de componentes críticos	√			√		
SA21	Evaluación de desarrolladores	√			√		
SA22	Componentes del sistema no compatibles	√			√		
SA23	Especialización	√			√		
SC.	**Protección de Sistemas y Comunicaciones**						
SC1	Política y procedimientos de protección del sistema y comunicaciones	√			√	√	
SC2	Separación del sistema y la funcionalidad del usuario		√		√	√	
SC3	Aislamiento de la función de seguridad		√		√	√	
SC4	Información en recursos del sistema compartido		√			√	
SC5	Protección de denegación de servicio		√			√	√
SC6	Disponibilidad de recursos		√		√	√	
SC7	Protección límite		√			√	√
SC8	Confidencialidad e integridad de la transmisión		√			√	√
SC10	Desconexión de la red		√			√	
SC11	Ruta de confianza		√		√		
SC12	Establecimiento y gestión de clave criptográfica			√		√	
SC13	Protección criptográfica		√			√	√
SC15	Dispositivos y aplicaciones informáticas colaborativas		√			√	
SC16	Transmisión de atributos de seguridad y privacidad		√				
SC17	Certificados de infraestructura de clave pública			√		√	
SC18	Código móvil	√				√	√
SC20	Servicio de resolución de nombre/dirección segura (fuente autoritaria)		√			√	
SC21	Servicio de resolución de nombre/dirección segura (resolución recursiva o de almacenamiento en caché)		√			√	
SC22	Arquitectura y aprovisionamiento para el servicio de resolución de nombre/dirección		√			√	
SC23	Autenticidad de la sesión		√			√	

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
SC24	Fallar en estado conocido		√		√	√	
SC25	Nodos delgados		√				
SC26	Señuelos		√				
SC27	Aplicaciones independientes de la plataforma		√				
SC28	Protección de la información en reposo		√			√	√
SC29	Heterogeneidad	√			√		
SC30	Ocultación y mala dirección	√			√		
SC31	Análisis de canal encubierto	√			√		√
SC32	División del sistema			√	√		
SC34	Programas ejecutables no modificables		√		√		
SC35	Identificación de código malicioso externo		√				
SC36	Procesamiento y almacenamiento distribuidos	√			√		
SC37	Canales fuera de banda	√			√		
SC38	Seguridad de las operaciones	√			√		
SC39	Aislamiento de procesos		√		√	√	
SC40	Protección de enlaces inalámbricos		√				
SC41	Acceso de dispositivo de puerto y E/S			√			
SC42	Capacidad y datos del sensor		√				
SC43	Restricciones de uso			√			
SC44	Cámaras de detonación		√				√
SC45	Sincronización del tiempo del sistema		√				
SC46	Aplicación de políticas de dominio cruzado		√				
SC47	Rutas de comunicaciones alternativas			√			
SC48	Reubicación del sensor			√			
SC49	Separación y aplicación de políticas controladas por hardware			√	√		
SC50	Separación y aplicación de políticas controladas por software			√	√		
SC51	Protección basada en hardware			√	√		
SI.	**Sistema e Integridad de la Información**						
SI1	Política y procedimientos de integridad del sistema e información	√			√	√	
SI2	Remediación de defectos	√				√	√
SI3	Protección de código malicioso			√		√	√
SI4	Monitoreo del sistema			√	√	√	√
SI5	Alertas de seguridad, avisos y directivas	√			√	√	√
SI6	Verificación de la función de seguridad y privacidad		√		√	√	
SI7	Integridad de software, firmware e información			√	√	√	
SI8	Protección contra el spam	√				√	
SI10	Validación de entrada de información		√		√	√	
SI11	Manejo de errores		√			√	
SI12	Gestión de la información y retención	√				√	

ID	FAMILIA	IMPLEMENTADO POR			GARANTÍA	AZURE	AWS
		o	s	o/s			
SI13	Prevención de fallas predecible	√			√		
SI14	No persistencia	√			√		
SI15	Filtrado de salida de información		√		√		
SI16	Protección de la memoria		√		√	√	
SI17	Procedimientos a prueba de fallas		√		√		
SI18	Operaciones de calidad de información de identificación personal			√			
SI19	Des-identificación			√			
SI20	Contaminación			√	√		
SI21	Actualizar la información			√	√		
SI22	Diversidad de información			√	√		
SI23	Fragmentación de información			√	√		
SR	**Gestión de Riesgos de la Cadena de Suministro**						
SR1	Política y procedimientos de gestión de riesgos de la cadena de suministro	√			√		
SR2	Plan de gestión de riesgos de la cadena de suministro	√			√		
SR3	Controles y procesos de la cadena de suministro			√	√		
SR4	Procedencia	√			√		
SR5	Estrategias, herramientas y métodos de adquisición	√			√		
SR6	Evaluaciones y revisiones de proveedores	√			√		
SR7	Seguridad de operaciones de la cadena de suministro	√			√		
SR8	Acuerdos de notificación	√			√		
SR9	Resistencia y detección de manipulaciones	√			√		
SR10	Inspección de sistemas o componentes	√			√		
SR11	Autenticidad componente	√			√		
SR12	Disposición de componentes	√			√		

Nota: Por el autor, basado en varias referencias.

Para elaborar la propuesta, se consideró los controles que presentan un resultado del promedio mayor al 50% en cada familia, en función de la comparativa realizada entre los recomendados por NIST 800-53 vs los aplicados por los proveedores de servicios de nube, Microsoft y Amazon; del resultado del mapeo se tiene como resultado las siguientes 11 familias:

- Concientización y Capacitación
- Auditoría y Rendición de Cuentas
- Evaluación, Autorización y Seguimiento
- Gestión de la configuración

- Planificación de contingencia
- Respuesta a Incidentes
- Mantenimiento
- Protección de medios
- Protección Física y Ambiental
- Evaluación de riesgos
- Sistema y Adquisición de Servicios

Sin embargo, a este resultado se consideró importante incluir 2 familias adicionales que son; Control de Acceso y Planificación, el primer control garantiza la seguridad de la data al limitar los accesos, mientras que el control Planificación, en la implementación de un proceso de seguridad es importante, ya que basado con el Ciclo de Deming este permite a las organizaciones establecer un enfoque estratégico al momento de definir los objetivos y prioridades de la organización.

Los controles de las familias que no se consideraron para esta propuesta se detallan a continuación, las cuales pueden incluirse en la definición de un programa de seguridad, dependiendo del alcance y objetivo de cada organización.

- Identificación y Autenticación
- Programas de Gestión
- Seguridad del personal
- PII Procesamiento y transparencia
- Protección de sistemas y comunicaciones
- Sistema e Integridad de la Información
- Gestión de riesgos de la cadena de suministro

Finalmente se tiene como resultado final el planteamiento de 141 controles, divididos en 13 familias que deben ser implementados por la empresa proveedora de servicios de nube para mejorar su postura de seguridad y ofrecer un nivel de protección más robusto a sus clientes. Además, se muestra una comparativa con los controles del estándar ISO 27001, esto es posible ya que la NIST 800-53 satisface la intención del requisito o control de seguridad asignado por la ISO 27001 de manera similar, como se muestra en la Tabla 4.

Tabla 4.
Análisis Final

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
AC.	**Control de Acceso**					
AC-1	Política y procedimientos de control de acceso	√	√	√		5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Administración de cuentas		√	√		A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Control de acceso		√	√		A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Control de flujo de información		√	√		A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separación de tareas		√	√		A.6.1.2
AC-6	Privilegios mínimos		√	√		A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Intentos de inicio de sesión sin éxito		√			A.9.4.2
AC-8	Notificación de uso del sistema		√		**48%**	A.9.4.2
AC-10	Control de sesión concurrente		√			None
AC-11	Bloqueo		√			A.11.2.8, A.11.2.9
AC-12	Terminación de la sesión		√			None
AC-14	Acciones permitidas sin identificación o autenticación		√			None
AC-16	Atributos de seguridad y privacidad		√	√		None
AC-17	Acceso remoto		√	√		A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Acceso inalámbrico		√	√		A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Control de acceso para dispositivos móviles		√	√		A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1
AC-20	Uso de sistemas externos		√	√		A.11.2.6, A.13.1.1, A.13.2.1
AC-21	El intercambio de información		√	√		None
AC-22	Contenido de acceso público		√			None
AC-25	Monitor de referencia	√				None
AT.	**Concientización y capacita**				**73%**	

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
AT1	Política y procedimientos de conciencia y capacitación	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT2	Entrenamiento y conciencia de alfabetización	√	√	√		7.3, A.7.2.2, A.12.2.1
AT3	Capacitación basada en roles	√	√	√		A.7.2.2*
AT4	Registros de entrenamiento	√	√			None
AT6	Comentarios de capacitación	√				None
AU.	**Auditoría y Rendición de Cuentas**					
AU1	Política y procedimientos de auditoría y responsabilidad	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU2	Registro de eventos		√			None
AU3	Contenido de registros de auditoría		√			A.12.4.1*
AU4	Capacidad de almacenamiento de registros de auditoría		√	√		A.12.1.3
AU5	Respuesta a las fallas del proceso de registro de auditoría		√			None
AU6	Revisión, análisis e informes de registros de auditoría	√	√	√	**53%**	A.12.4.1, A.16.1.2, A.16.1.4
AU7	Reducción de registros de auditoría y generación de informes	√	√	√		None
AU8	Marcas de tiempo		√			A.12.4.4
AU9	Protección de información de auditoría		√			A.12.4.2, A.12.4.3, A.18.1.3
AU10	No repudio	√	√			None
AU11	Retención de registros de auditoría	√	√			A.12.4.1, A.16.1.7
AU12	Generación de registros de auditoría		√	√		A.12.4.1, A.12.4.3
AU13	Monitoreo de la divulgación de información	√		√		None
AU14	Auditoría	√				A.12.4.1*
CA.	**Evaluación, Autorización y Seguimiento**					
CA1	Políticas y procedimientos de evaluación y autorización	√	√		**88%**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA2	Evaluaciones de control	√	√	√		A.14.2.8, A.18.2.2, A.18.2.3
CA3	Intercambio de información	√	√	√		A.13.1.2, A.13.2.1, A.13.2.2

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
CA5	Plan de acción e hitos	√	√			8.3, 9.2, 10.1*
CA6	Autorización	√	√			9.3*
CA7	Monitoreo continuo	√	√	√		9.1, 9.2, A.18.2.2, A.18.2.3*
CA8	Pruebas de penetración	√	√	√		None
CA9	Conexiones internas del sistema	√	√	√		None
CM.	**Gestión de la Configuración**					
CM1	Política y procedimientos de gestión de configuración	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM2	Configuración de línea de base	√	√	√		None
CM3	Control de cambio de configuración	√	√	√		8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM4	Análisis de impacto	√	√	√		A.14.2.3
CM5	Restricciones de acceso para el cambio		√	√	**67%**	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM6	Ajustes de configuración		√	√		None
CM7	Menos funcionalidad		√	√		A.12.5.1*
CM8	Inventario de componentes del sistema	√	√	√		A.8.1.1, A.8.1.2
CM9	Plan de gestión de configuración		√	√		A.6.1.1*
CM10	Restricciones de uso de software		√	√		A.18.1.2
CM11	Software instalado por el usuario		√	√		A.12.5.1, A.12.6.2
CM12	Ubicación de información	√				None
CM14	Componentes firmados	√				None
CP.	**Planificación de Contingencia**					
CP1	Política y procedimientos de planificación de contingencia	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP2	Plan de contingencia		√	√	**58%**	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1
CP3	Capacitación de contingencia	√	√	√		A.7.2.2*
CP4	Prueba del plan de contingencia	√	√	√		A.17.1.3
CP6	Sitio de almacenamiento alternativo		√	√		A.11.1.4, A.17.1.2, A.17.2.1
CP7	Sitio de procesamiento alternativo		√			A.11.1.4, A.17.1.2, A.17.2.1

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
CP8	Servicios de telecomunicaciones		√	√		A.11.2.2, A.17.1.2
CP9	Copia de seguridad del sistema		√	√		A.12.3.1, A.17.1.2, A.18.1.3
CP10	Recuperación del sistema y reconstitución		√	√		A.17.1.2
CP11	Protocolos de comunicaciones alternativos			√		A.17.1.2*
CP12	Modo seguro	√				None
IR.	**Respuesta Incidentes**					
IR1	Política y procedimientos de respuesta a incidentes	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR2	Entrenamiento de respuesta a incidentes	√	√			A.7.2.2*
IR3	Prueba de respuesta a incidentes	√	√	√		None
IR4	Manejo de incidentes		√	√	**67%**	A.16.1.4, A.16.1.5, A.16.1.6
IR5	Monitoreo de incidentes	√	√	√		None
IR6	Informe de incidentes		√	√		A.6.1.3, A.16.1.2
IR7	Asistencia de respuesta a incidentes		√			None
IR8	Plan de respuesta a incidentes		√	√		7.5.1, 7.5.2, 7.5.3, A.16.1.1
IR9	Respuesta del derrame de información		√			None
MA.	**Mantenimiento**					
MA1	Política y procedimientos de mantenimiento del sistema	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA2	Mantenimiento controlado		√	√	**53%**	A.11.2.4*, A.11.2.5*
MA3	Herramientas de mantenimiento		√	√		None
MA4	Mantenimiento no local		√	√		None
MA5	Personal de mantenimiento		√	√		None
MA6	Mantenimiento oportuno		√			A.11.2.4
MP.	**Protección de Medios**					
MP1	Política y procedimientos de protección de medios	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP2	Acceso a los medios		√	√	**54%**	A.8.2.3, A.8.3.1, A.11.2.9
MP3	Marcado de medios		√			A.8.2.2
MP4	Almacén de datos		√	√		A.8.2.3, A.8.3.1, A.11.2.9

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
MP5	Transporte de medios		√	√		A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP6	Desinfeción de medios		√	√		A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
MP7	Uso de los medios		√	√		A.8.2.3, A.8.3.1
PE.	**Protección Física y Ambiental**					
PE1	Política y procedimientos de protección física y ambiental	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE2	Autorizaciones de acceso físico		√	√		A.11.1.2*
PE3	Control de acceso físico		√	√		A.11.1.1, A.11.1.2, A.11.1.3
PE4	Control de acceso para medio de transmisión		√	√		A.11.1.2, A.11.2.3
PE5	Control de acceso para dispositivos de salida		√	√		A.11.1.2, A.11.1.3
PE6	Monitoreo de acceso físico	√	√	√		None
PE8	Registros de acceso a los visitantes	√	√			None
PE9	Equipo de energía y cableado		√	√	**55%**	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE10	Cierre de emergencia		√	√		A.11.2.2*
PE11	Potencia de emergencia		√	√		A.11.2.2
PE12	Iluminación de emergencia		√	√		A.11.2.2*
PE13	Protección contra incendios		√	√		A.11.1.4, A.11.2.1
PE14	Controles ambientales		√	√		A.11.1.4, A.11.2.1, A.11.2.2
PE15	Protección de daños por agua		√	√		A.11.1.4, A.11.2.1, A.11.2.2
PE16	Entrega y eliminación		√	√		A.8.2.3, A.11.1.6, A.11.2.5
PE17	Sitio de trabajo alternativo		√			A.6.2.2, A.11.2.6, A.13.2.1
PE18	Ubicación de los componentes del sistema		√	√		A.8.2.3, A.11.1.4, A.11.2.1
PE19	Fugas de información			√		A.11.1.4, A.11.2.1
PE20	Monitoreo y seguimiento de activos			√		A.8.2.3*
PL.	**Planificación**					
PL1	Política y procedimientos de planificación	√	√		**46%**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL2	Planes de seguridad y privacidad del sistema	√	√	√		7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1

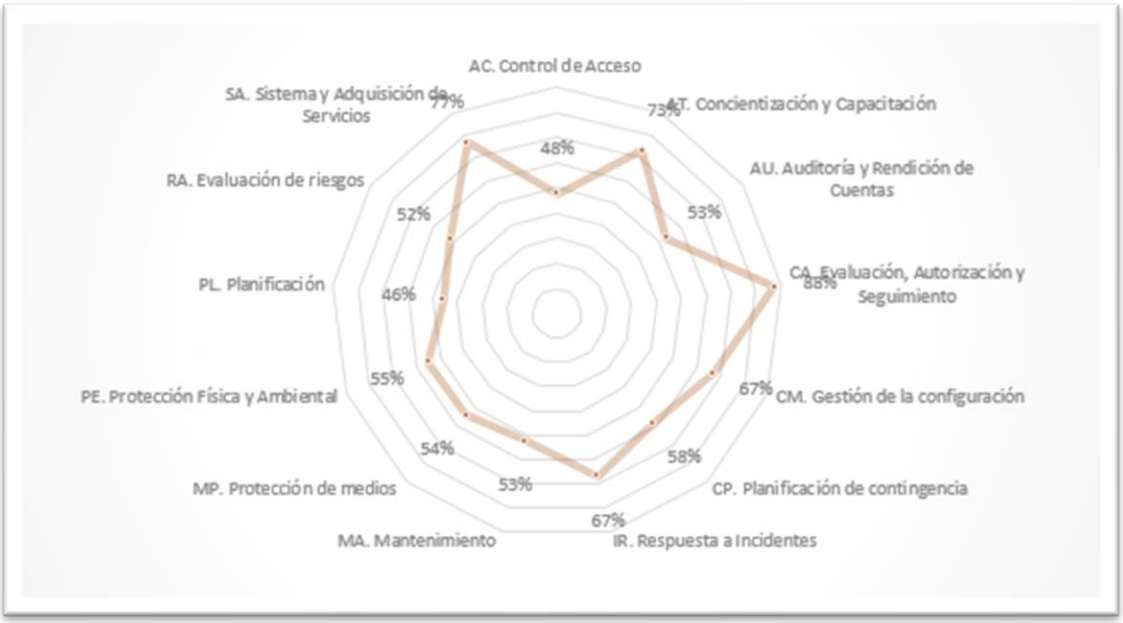
ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
PL4	Reglas de comportamiento	√	√			A.7.1.2, A.7.2.1, A.8.1.3
PL8	Arquitecturas de seguridad y privacidad	√	√	√		A.14.1.1*
PL9	Gestión central	√				None
RA.	**Evaluación de Riesgos**					
RA1	Política y procedimientos de evaluación de riesgos	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA2	Categorización de seguridad		√	√		A.8.2.1
RA3	Evaluación de riesgos	√	√	√	**52%**	6.1.2, 8.2, A.12.6.1*
RA5	Monitoreo y escaneo de vulnerabilidad	√	√	√		A.12.6.1*
RA6	Encuesta de contramedidas de vigilancia técnica	√				None
RA7	Respuesta a los riesgos	√				6.1.3, 8.3, 10.1
RA8	Evaluaciones de impacto de la privacidad	√				None
RA10	Caza de amenazas	√				None
SA.	**Sistema y Adquisición de Servicios**					
SA1	Política y procedimientos de adquisición de sistemas y servicios	√	√			5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA2	Asignación de recursos	√	√			None
SA3	Ciclo de vida de desarrollo de sistemas	√	√	√		A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA4	Proceso de adquisición	√	√	√		8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA5	Documentación del sistema	√	√	√	**77%**	7.5.1, 7.5.2, 7.5.3, A.12.1.1*
SA8	Principios de ingeniería de seguridad	√	√	√		A.14.2.5
SA9	Servicios de sistema externo	√	√	√		A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA10	Gestión de configuración del desarrollador	√	√	√		A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA11	Prueba y evaluación del desarrollador	√	√	√		A.14.2.7, A.14.2.8
SA15	Proceso de desarrollo, estándares y herramientas	√	√	√		A.6.1.5, A.14.2.1
SA16	Capacitación proporcionada por el desarrollador	√	√			None

ID	FAMILIA	GARANTÍA	AZURE	AWS	PROMEDIO	ISO/IEC 27001
SA17	Seguridad de desarrollador y arquitectura y diseño de privacidad	√	√	√		A.14.2.1, A.14.2.5
SA20	Desarrollo personalizado de componentes críticos	√				None
SA21	Evaluación de desarrolladores	√				A.7.1.1
SA22	Componentes del sistema no compatibles	√				None
SA23	Especialización	√				None

Nota: Por el autor, basado en varias referencias

La Figura 3 muestra el nivel de la implementación de los controles de cada familia de la propuesta, de acuerdo con los resultados detallados en la tabla 4.

Figura 3.
Nivel de Implementación de controles por Familia



Nota: Por el autor, basado en los resultados de la tabla 4

Es importante considerar que la seguridad en entornos de nube es una responsabilidad compartida entre el proveedor y el usuario, por lo que los controles propuestos también deben alinearse con los requisitos y objetivos de cada cliente.

CAPÍTULO II: PROPUESTA

La propuesta se realizó tomando como referencia la comparación entre los controles de NIST 800-53 y los aplicados por dos de los proveedores más destacados de servicios en la nube, donde se obtuvo controles de trece familias que podrían servir como punto de partida para la creación de nuevos programas de seguridad o como herramienta para la optimización de programas ya existentes.

2.1. Fundamentos teóricos aplicados

A continuación, se detallan los fundamentos teóricos para el presente proyecto.

2.1.1. Amenazas de seguridad más comunes en entornos de nube

Según Ramírez et al., (2017) la adopción de servicios en la nube trae consigo la aparición de nuevas vulnerabilidades de seguridad que pueden comprometer los beneficios alcanzados en la adopción de tecnologías basadas en la nube. Entre las principales amenazas se tiene:

- Fuga de Información
- Credenciales comprometidas y suplantación en la autenticación
- Interfaces y API hackeadas
- Vulnerabilidades del Sistema o Bugs Explotables en los programas
- Secuestro de cuentas
- Intrusos maliciosos
- Amenazas Persistentes Avanzadas (APT)
- Pérdida permanente de la data
- Inadecuada Diligencia
- Abuso de los servicios de Nube
- Ataques DoS
- Tecnología compartida, peligros compartidos

Así también según Potluri, et al (2021), en la tabla 5, se muestran los ataques observados en la computación en la nube.

Tabla 5.
Ataques en la Computación en la Nube

Ataques	
Funcionalidad de abuso	Técnicas probabilísticas
Ataque a la estructura de datos	Manipulación de protocolos
Código malicioso incrustado	Agotamiento de recursos
Explotación de la autenticación.	Manipulación de recursos
Injection	Ataque Sniffing
Ataque transversal de ruta	Ataque spoofing

Nota: Tomado de Cloud Security Techniques and Applications

2.1.2. Marcos y Estándares de Seguridad

Los activos de información son la parte más importante de las organizaciones, por lo que es necesario contar con un estándar de seguridad adecuado que permita aplicar las medidas de seguridad a implementar de acuerdo con las mejores prácticas y estándares de seguridad los cuales pueden estar basado en los diferentes marcos de seguridad, de acuerdo con Barry (2013), muchos de los estándares establecen los requisitos de formas ligeramente diferentes, como son Organización Internacional de Normalización (ISO), Instituto Nacional de Estándares y Tecnología (NIST), Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas (COBIT), Biblioteca de Infraestructura de Tecnología de la Información (ITIL), Marco de Control de Ciberseguridad (CCM), Payment Card Industry Data Security Standard (PCI DSS), entre otros los cuales permiten identificar, detectar, responder y recuperarse de amenazas.

2.1.3. Marco de Ciberseguridad del NIST

De acuerdo con la OEA y AWS (2019), el Marco de Ciberseguridad consiste en un conjunto de acciones con resultados previstos en términos de seguridad, estos resultados se encuentran estructurados en Categorías y alineados con Referencias Informativas basadas en estándares reconocidos en la industria.

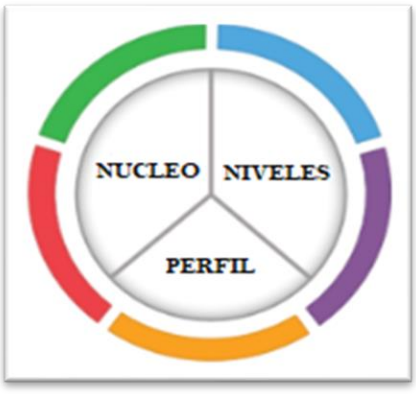
Según NIST (2018), el marco de ciberseguridad NIST permite a cualquier tipo de organización comprender, gestionar y reducir los riesgos de seguridad informática gracias a la flexibilidad en la implementación de controles para la protección de datos.

Es importante aclarar que el marco de ciberseguridad de NIST no reemplaza el programa de seguridad o gestión de riesgos de una organización; más bien, complementa los programas existentes y proporciona valor al servir como un instrumento avanzado de gestión y evaluación de riesgos y seguridad.

El marco proporciona la oportunidad de fortalecer la seguridad de la infraestructura crítica de una entidad, ya que se basa en procesos y controles delineados por estándares de ciberseguridad como son: NIST SP 800-53, ISO/IEC 27001:2013, COBIT 5 entre otros, unificando así los estándares de ciberseguridad; con un enfoque diseñado para reducir los riesgos asociados a las posibles amenazas informáticas que pueden poner el peligro la seguridad de la información y apoyar a las organizaciones a comprender mejor los riesgos a los que se encuentran expuestos, brinda una guía de mejores prácticas para realizar una administración correcta, reducir los riesgos y proteger los datos.

El marco de ciberseguridad desarrollado por NIST (2018) es adecuado para cualquier organización que aspire implementar o mejorar su sistema de seguridad, este actúa como una interconexión para facilitar la comunicación entre equipos multidisciplinarios utilizando un lenguaje claro y comprensible, sin términos técnicos complejos; está conformado por tres componentes principales que son: núcleo, niveles de implementación y perfil.

Figura 4.
Marco Ciberseguridad del NIST



Nota: Tomado de Marco Ciberseguridad del NIST

a) Núcleo

Es un conjunto de acciones y logros objetivos, organizados por categoría y alineados con referencias informativas, incluye cinco funciones simultáneas y secuenciales de alto nivel que son:

- Identificar
- Proteger
- Detectar
- Responder
- Recuperar

Estas funciones no solo son válidas para la administración de riesgos de seguridad informática, también son aplicables a la gestión de riesgos en general.

Figura 5.
Funciones de Marco Ciberseguridad del NIST

Nota: Tomado de Marco Ciberseguridad del NIST

Las cinco funciones están compuestas por 23 categorías divididas entre las cinco funciones.

Figura 6.
Categorías de NIST Cibersecurity Framework

ID Identificar	PR Proteger	DE Detectar	RS Responder	RC Recuperar
ID.AM - Gestión de Activos ID.BE - Entorno empresarial ID.GV - Gobernanza ID.RA - Evaluación de riesgos ID.RM - Estrategia de Gestión de Riesgos ID.SC - Gestión de riesgos de la cadena de suministro	PR.AC - Gestión de Identidad y Control de Acceso PR.AT - Sensibilización y Formación PR.DS - Seguridad de datos PR.IP - Procesos y Procedimientos de Protección de la Información PR.MA - Mantenimiento PR.PT - Tecnología de Protección	DE.AE - Anomalías y eventos DE.CM - Monitoreo Continuo de Seguridad DE.DP - Detección de Procesos	RS.RP - Planificación de respuesta RS.CO - Comunicaciones RS.AN - Análisis RS.MI - Mitigación RS.IM - Mejoras	RC.RP - Planificación de recuperación RC.IM - Mejoras RC.CO - Comunicaciones

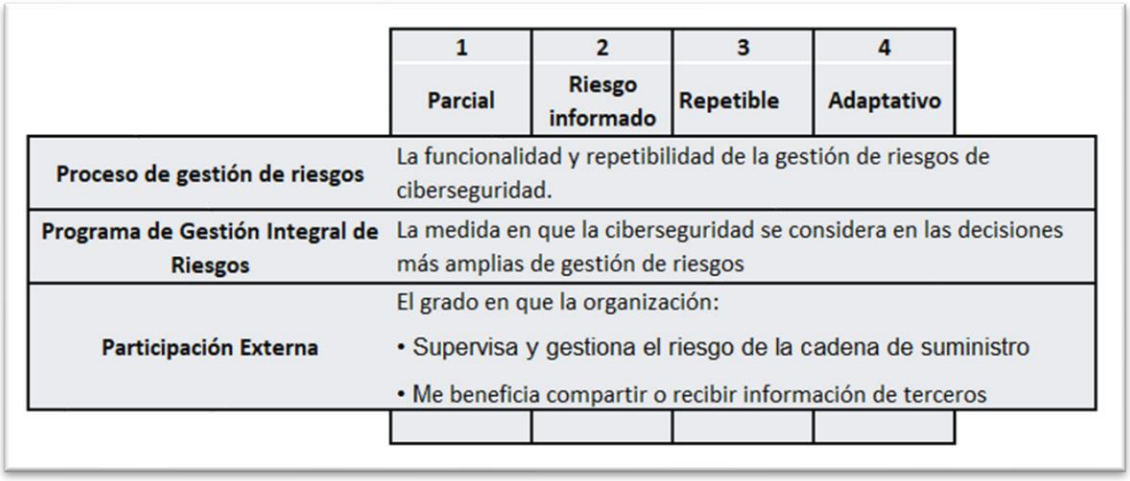
Nota: Por el autor, basado en varias referencias

Las categorías corresponden a un nivel más profundo de abstracción en el núcleo y constan de 108 subcategorías, que son afirmaciones fundamentadas en los logros que proporcionan directrices para establecer o perfeccionar un programa de seguridad de la información, permite una implementación basada en el riesgo que se determinen según las necesidades de la organización, ya que el sistema está enfocado en resultados y no establece el método que la organización debe seguir para alcanzar dichos resultados.

b) Niveles de Implementación

Brinda a las organizaciones un entorno sobre cómo abordar la gestión de riesgos de seguridad informática a través de niveles, estos niveles ayudan a las organizaciones a considerar el nivel apropiado de rigor para sus programas de seguridad cibernética y, a menudo, se usan como una herramienta de comunicación para analizar el apetito al riesgo, las prioridades de la misión y los presupuestos. Los niveles van desde nivel 1 - Parcial hasta nivel 4 – Adaptativo, de acuerdo a la figura 7.

Figura 7.
Niveles de implementación de NIST Cibersecurity Framework



	1 Parcial	2 Riesgo informado	3 Repetible	4 Adaptativo
Proceso de gestión de riesgos	La funcionalidad y repetibilidad de la gestión de riesgos de ciberseguridad.			
Programa de Gestión Integral de Riesgos	La medida en que la ciberseguridad se considera en las decisiones más amplias de gestión de riesgos			
Participación Externa	El grado en que la organización: • Supervisa y gestiona el riesgo de la cadena de suministro • Me beneficia compartir o recibir información de terceros			

Nota: Tomado de Marco Ciberseguridad del NIST

c) Perfiles

Permite alinear funciones, categorías y subcategorías con las necesidades comerciales, objetivos organizacionales, tolerancia al riesgo, y los recursos con los resultados previstos en el Núcleo del Marco.

Estos perfiles se utilizan para detallar el estado actual y el estado objetivo de las operaciones de ciberseguridad. En el perfil actual se describen los resultados obtenidos, mientras que en el perfil objetivo se muestran los resultados esenciales para alcanzar las metas establecidas en la gestión del riesgo.

2.1.4. Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) según la ISO/IEC 27001 abarca un conjunto de políticas, procedimientos y directrices, para llevar a cabo la implementación, operación, supervisión, auditoría, mantenimiento y mejora continua en la seguridad de los activos de información. De acuerdo con este estándar, el objetivo es mantener la confidencialidad, la integridad y la disponibilidad de la información, a través del análisis y valoración de los activos de información se realiza de acuerdo con estas tres condiciones.

2.1.5. ISO 27001

Según la ISO/IEC (2013), el estándar 27001 provee las directrices y buenas prácticas de administración de la seguridad de la información de una organización, incorpora la selección, implementación y gestión de controles considerando el entorno de riesgo de la organización. El estándar está basado en una secuencia de fundamentos de gestión de calidad, que incorpora una clara orientación al cliente, la implicación y participación de la alta dirección y un enfoque basado en procesos y mejora continua.

ISO 27001 está confirmada por once secciones y un anexo que contiene 114 controles divididos entre 14 dominios, las partes 0 a 3 son introductorias y opcionales; y de forma obligatoria las secciones de 4 a 10, esto significa que las organizaciones deben implementar todos los requisitos para cumplir con el estándar. Los controles a los que se hace referencia en el Anexo A, solo deben llevarse cumplirse si se establece que son relevantes para la declaración de aplicabilidad.

Los 14 dominios del Anexo A de la ISO 27001 se encuentra clasificados:

- Políticas de seguridad de la Información
- Organización de la seguridad de la información
- Seguridad de los Recursos Humanos
- Gestión de recursos
- Control de Acceso
- Criptografía
- Seguridad física y ambiental
- Seguridad Operacional
- Seguridad de las Comunicaciones
- Adquisición, desarrollo y mantenimiento de Sistemas
- Relaciones con los proveedores

- Gestión de Incidentes en Seguridad de la Información
- Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio
- Cumplimiento

Cada organización debe elegir la metodología que mejor se adapte a sus necesidades, es esencial comprender que no se limita al campo técnico, ya que también incluye áreas como recursos humanos, seguridad financiera, comunicación, etc., el control es obligatorio, según corresponda en cada organización.

2.1.6. NIST 800-53

NIST 800-53 es un catálogo de controles de seguridad y privacidad destinados a todos los sistemas de información federales de EE. UU, los controles de seguridad y privacidad descritos en esta publicación tienen una organización bien definida y estructurada para facilitar su uso en el proceso de especificación y selección de controles de seguridad y privacidad, de acuerdo con NIST SP 800-53 (2020).

Los controles están organizados en veinte familias, cada familia contiene controles que están relacionados con el tema específico de cada familia. Los controles de seguridad y privacidad pueden involucrar aspectos de política, fiscalización, supervisión, procesos manuales y mecanismos automatizados. La siguiente tabla enumera las familias de control de seguridad y privacidad y sus identificadores de familia asociados.

Tabla 6.
Familias de NIST 800-53

Id	Familia	Id	Familia
AC	Control de Acceso	PE	Protección Física y Ambiental
AT	Concientización y Capacitación	PL	Planificación
AU	Auditoría y Rendición de Cuentas	PM	Programas de Gestión
CA	Evaluación, Autorización y Seguimiento	PS	Seguridad del personal
CM	Gestión de la configuración	PT	PII Procesamiento y transparencia
CP	Planificación de contingencia	RA	Evaluación de riesgos
IA	Identificación y Autenticación	SA	Sistema y Adquisición de Servicios
IR	Respuesta a Incidentes	SC	Protección de sistemas y comunicaciones
MA	Mantenimiento	SI	Sistema e Integridad de la Información

MP	Protección de medios	SR	Gestión de riesgos de la cadena de suministro

Nota: Tomado de NIST SP 800-53

2.2. Descripción de la propuesta

La ISO 27001 es considerada una norma amplia que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en general y no se enfoca específicamente en la seguridad en la nube. Sin embargo, en el año 2015 con la publicación de la extensión ISO 27017 abordó aspectos específicos de la seguridad de la información en la nube.

A comparación con NIST, al estar involucrada en la investigación y desarrollo de la nube, fue uno de los pioneros en definir y estandarizar conceptos relacionados con la computación en la nube; NIST a través de su publicación especial NIST 800-145 del año 2011, estableció un conjunto de características y modelos de servicio para la esta tecnología. Así también ha desarrollado otros documentos y guías específicas para la seguridad en la nube, como el "NIST Cloud Computing Security Reference Architecture" y el "NIST Cloud Computing Synopsis and Recommendations". Estos documentos proporcionan una orientación más detallada sobre la seguridad en la nube, los mismos que se pueden complementar con la implementación de los controles de la NIST SP 800-53.

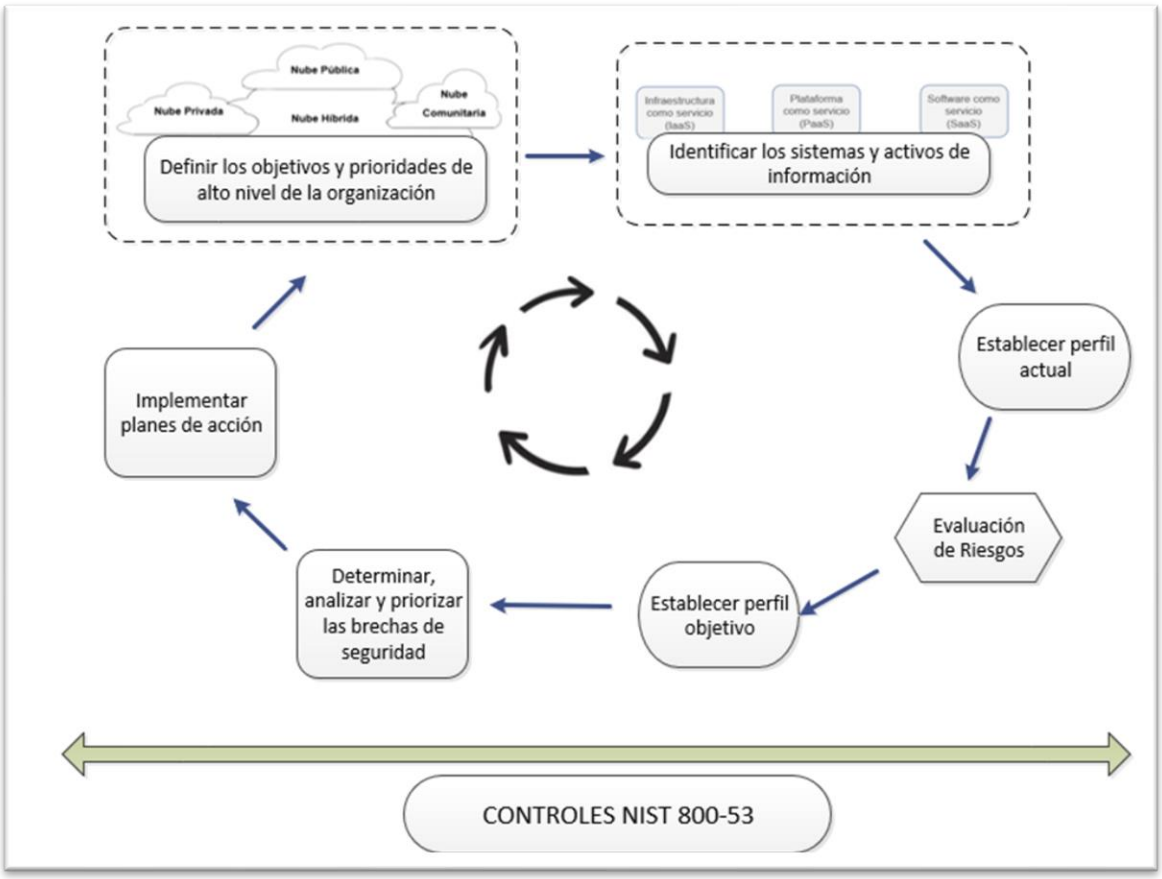
NIST ofrece una orientación práctica y detallada para implementar controles de seguridad, con la que las organizaciones pueden proteger sus sistemas en la nube, proporcionando una serie de pautas y recomendaciones que ayudan a identificar, proteger, detectar, responder y recuperarse de las amenazas presentes en los sistemas de la nube.

a) Estructura general

El Marco Ciberseguridad del NIST es considerado como una herramienta que posibilita a las organizaciones administrar los riesgos de seguridad informática de forma flexible y adaptable a su realidad, ya que plantea varias estrategias que puede ser aplicable según la necesidad de cada empresa. De acuerdo con el Programa Federal de Administración de Riesgos y Autorizaciones de EE. UU. (FedRAMP) entre sus objetivos tiene acelerar la adopción de soluciones seguras, proporcionar una visión estandarizada para evaluar, monitorear y autorizar productos y servicios en la nube.

La presente propuesta está basada en una estrategia de 7 pasos a considerar para la implementación del Marco Ciberseguridad del NIST y complementada con la aplicación de 13 familias de NIST 800-53 definidas como resultado del mapeo, cada familia contiene controles que están relacionados con un tema específico para garantizar la seguridad y privacidad de la información en los servicios de nube. Es fundamental considerar que cualquier sistema de seguridad implementado, debe estar vinculado a un proceso de mejora continua, esto le permita identificar y proponer acciones de mejora para garantizar la seguridad de la información.

Figura 8.
Estructura General de la Propuesta



Nota: Por el autor, basado en varias referencias

b) Explicación del aporte

El Marco Ciberseguridad del NIST es una parte clave dentro de un proceso de gestión de seguridad, pudiendo ser la base para la creación de nuevos programas de seguridad o como herramienta para mejorar programas ya establecidos, debido a que su objetivo no es reemplazar los procesos de eguridad existentes de las organizaciones, sino para identificar las brechas de seguridad en su enfoque actual y

crear un plan de acción para lograr la mejora continua en la protección de la información y la adaptación a los desafíos de seguridad que están en constante evolución.

La estrategia de Establecimiento o Mejora de un Programa de Ciberseguridad planteada por el Core Framework de la NIST (2018) se complementa con las 13 familias identificadas previamente:

I. **Priorizar y determinar el alcance. -** Determinar los objetivos estratégicos y las prioridades de mayor importancia de la organización.
   - Planificación (PL)

II. **Orientación. -** Establecer los sistemas y activos que se encuentran relacionados con el alcance, los requisitos legales o normativos y el enfoque de riesgo global.
   - Concientización y Capacitación (AT)

III. **Establecer perfil actual. -** Realizar una evaluación del programa de seguridad de la información con el fin de crear un perfil inicial. Es fundamental que esta evaluación abaque la cantidad de personas, roles de trabajo, capacitación de procesos y políticas referentes a sistemas información, capacidades, configuraciones, vulnerabilidades, actualizaciones, operaciones, contratos de soporte, etc.
   - Evaluación, Autorización y Seguimiento (CA)
   - Gestión de la Configuración (CM)

IV. **Realizar una evaluación de riesgos. -** Evaluar el entorno operativo que permita determinar la probabilidad de que se presente un incidente de ciberseguridad y estimar el impacto que podría tener en la organización.
   - Control de Evaluación de Riesgos (RA)

V. **Crear un perfil objetivo. –** Establecer los resultados deseados en términos de seguridad de la información que se buscan para la organización, considerando la misión y los objetivos comerciales establecidos, además los requisitos vinculados a cumplimiento normativo y legal.
   - Control de Sistema y Adquisición de Servicios (SA)

- Control de Acceso (AC)

VI. **Determinar, analizar y priorizar las brechas. –** En esta etapa se debe realizar una comparativa entre el Perfil Actual y el Perfil Objetivo esto permitirá determinar las brechas de seguridad. Posterior crear un plan de acción priorizando la atención de las brechas identificadas, en este paso también se debe considerar los recursos necesarios, que incluyen los recursos financieros y personal necesario.

- Evaluación de Riesgos (RA)
- Control de Planificación (PL)
- Control de Auditoría y Rendición de Cuentas (AU)

VII. **Implementar el plan de acción. -** Determinar las acciones que se deben tener en cuenta para atender las brechas de seguridad identificadas para llegar al Perfil Objetivo planteado. Es fundamental que las medidas adoptadas contemplen todos los aspectos de gobernanza, tecnología y procesos.

- Control de Acceso (AC)
- Control de Gestión de la Configuración (CM)
- Control de Respuesta a Incidentes (IR)
- Control de Mantenimiento (MA)
- Control de Protección de Medios (MP)
- Control de Protección Física y Ambiental (PE)
- Planificación de Contingencia (CP)

Es importante recordar que esta propuesta es solo una sugerencia y que los controles específicos a implementar pueden variar según las necesidades y requisitos de seguridad de cada organización.

c) Estrategias o técnicas

En la tabla 7 se detalla las técnicas que podrían ser implementadas en cada familia definida previamente.

Tabla 7.
Estrategia de Implementación.

PASOS	FAMILIA
Priorizar y determinar el alcance	Planificación (PL) Mantener reuniones con la alta dirección de la organización, donde se identifique los objetivos, prioridades y alcance de la organización para la implementación de controles de seguridad en la nube basados en NIST 800-53.
Orientación	Concientización y Capacitación (AT) Definir planes de capacitación para el personal de la organización, donde se abarque temas como activos de información relacionados con el alcance del proyecto, los requisitos legales y regulatorios a cumplir, los riesgos, amenazas a los cuales se encuentran expuestos, las mejores prácticas de seguridad, y la importancia del cumplimiento de los controles de seguridad de NIST 800-53 basados en políticas y procedimientos de la organización.
Establecer perfil actual	Evaluación, Autorización y Seguimiento (CA) Realizar una evaluación completa del sistema de seguridad en la nube para crear el perfil actual de la organización, este debe incluir, procesos, políticas, capacidades, configuraciones, vulnerabilidades y operaciones relacionadas con la nube. Gestión de la Configuración (CM) Establecer una línea base de configuración para los servicios en la nube y garantizar que los cambios estén bien documentados, a través de políticas y procedimientos.
Realizar una evaluación de riesgos	Evaluación de Riesgos (RA) Realizar un análisis al entorno operativo de los servicios de nube que permita identificar la probabilidad de eventos de seguridad y el impacto que tendría en el proveedor y sus clientes. Esto permitirá priorizar las acciones y decisiones en función de los riesgos más significativos.
Crear un perfil objetivo	Sistema y Adquisición de Servicios (SA) Establecer un perfil objetivo donde se incluya los resultados esperados de seguridad para los servicios de nube, los mismos que deben estar alineados con los objetivos y alcance de la organización, así como los requisitos legales y normativos. También es importante identificar los servicios, sistemas y recursos necesarios para lograr los resultados esperados.

PASOS	FAMILIA
	Control de Acceso (AC) Establecer el perfil objetivo de seguridad para el acceso a la nube, incluyendo controles de acceso necesarios para alcanzar un nivel adecuado de seguridad y protección de la información
Determinar, analizar y priorizar las brechas	Evaluación de Riesgos (RA) Comparar el perfil actual con el perfil objetivo, posibilitará la identificación de las deficiencias de seguridad existentes y así priorizar las acciones a tomar y establecer un plan de acción. Planificación (PL) Con base al resultado de la Evaluación de Riesgos (RA) se debe crear un plan de acción para mitigarlas, incluyendo los recursos necesarios para llevar a cabo las acciones requeridas. Auditoría y Rendición de Cuentas (AU) Evaluar la efectividad de los controles implementados mediante auditorías y la revisión de registros para identificar áreas de mejora y priorizar acciones correctivas.
Implementar el plan de acción	Control de Acceso (AC) Establecer políticas y mecanismos para controlar el acceso a los recursos y datos en la nube, incluyendo mecanismos de control de acceso como pueden ser: Múltiple factor de autenticación (MFA), roles basados en políticas (RBAC), cifrado de datos, entre otros. Gestión de la Configuración (CM) Asegurar que los cambios en las configuraciones de los sistemas de nube estén documentados y autorizados, a través de la implementación de políticas y procedimientos. Respuesta a Incidentes (IR) Definir un plan de respuesta a incidentes en la nube con la aplicación de procedimientos para mitigar y recuperarse de eventos adversos en la nube. Mantenimiento (MA) Mantener y actualizar regularmente los sistemas y aplicaciones en la nube para abordar vulnerabilidades y asegurar que estén protegidos contra amenazas. Protección de Medios (MP) Implementar medidas para proteger los medios físicos y digitales que almacenan o procesan datos en la nube.

PASOS	FAMILIA
	Protección Física y Ambiental (PE) Implementar medidas para proteger los recursos físicos de la nube, como centros de datos y servidores, contra acceso no autorizado y daños físicos.
	Planificación de Contingencia (CP) Definir el plan de acción para eventos de seguridad que afecten al normal funcionamiento del servicio, esto implica establecer procedimientos detallados para responder a incidentes de seguridad, así como desarrollar planes de continuidad del negocio en caso de desastres.

Nota: Por el autor, basado en varias referencias

2.3. Valoración de la propuesta

La propuesta planteada ha sido revisada por tres expertos de diferentes áreas de tecnología, teniendo como resultado que la propuesta presentada ofrece una guía sólida y coherente para abordar los desafíos de seguridad en entornos de nube, ya que al tener un enfoque en la identificación, evaluación y mitigación, junto con la alineación con estándares reconocidos como NIST e ISO, la convierten en una herramienta válida para cualquier organización que busque garantizar la protección de la información en entornos de nube.

El respaldo otorgado por los expertos resalta la pertinencia y el valor de la propuesta, que sin duda constituye una herramienta para las organizaciones que buscan establecer una estrategia de seguridad en entornos de nube. Su alineación con estándares reconocidos, su enfoque en la acción preventiva y su capacidad de adaptarse a los cambios tecnológicos hacen de esta propuesta una guía esencial en la búsqueda de la seguridad y protección de la información en el entorno dinámico de la nube.

2.4. Matriz de articulación de la propuesta

En la matriz se resume la articulación del producto desarrollado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos que han sido utilizados.

Tabla 8.
Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Computación en la Nube	Sistema que permite acceder a recursos informáticos, como almacenamiento, procesamiento, redes, aplicaciones y servicios, desde cualquier ubicación (NIST SP 800-145, 2011).	Investigación Bibliográfica	Identificar las características de la computación en la nube.	Analizar Conceptos	NIST SP 800-145
Principales modelos de servicio	Se define 3 principales modelos de servicios en la nube que son: • SaaS - Software como servicio • PaaS - Plataforma como servicio • IaaS - Infraestructura como servicio (NIST SP 800-145, 2011)	Investigación Bibliográfica	Servicios principales de nube	Analizar Conceptos	NIST SP 800-145
Marco de Ciberseguridad del NIST	Es un conjunto de actividades, con resultados esperados en términos de ciberseguridad, los cuales se encuentran estructurados en Categorías	Investigación Bibliográfica	Guía de ciberseguridad basado en cinco funciones principales, Identificar, Proteger,	Creación de un programa de seguridad o como herramienta	Cybersecurity Framework (CSF) 2.0

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
	y alineados con Referencias Informativas basadas en estándares reconocidos en la industria. (OEA y AWS, 2019)		Detectar, Responder y Recuperar, que proporcionan una base sólida para desarrollar estrategias de ciberseguridad.	para la mejora de un programa existente.	
NIST SP 800-53	Es un catálogo de controles de seguridad y privacidad destinados a todos los sistemas de información federales de EE. UU, los controles de seguridad y privacidad descritos en esta publicación tienen una organización bien definida y estructura. (NIST SP 800-53, 2020)	Investigación Bibliográfica	Lista de controles de ciberseguridad, basado en 20 familias, que se pueden utilizar como parte de una estrategia de ciberseguridad.	Mejorar la seguridad en entornos de nube.	NIST SP 800-53, ISO27001

Nota: Por el autor, basado en varias fuentes.

CONCLUSIONES

- Asegurar la información en cualquier tipo organización es una tarea compleja, por lo que la integración de estándares, marcos de referencia y buenas prácticas empleadas por proveedores de servicios en la nube ha permitido establecer una propuesta de controles de seguridad para identificar, proteger, detectar, responder y recuperarse en entornos de nube.

- Con la revisión del estado del arte sobre la seguridad en la nube, se identificaron diversas buenas prácticas aplicadas por proveedores de servicios en la nube más influyentes.

- La comparación detallada entre los marcos y estándares de referencia, del NIST 800-53 y la familia ISO-27000, permitió identificar puntos de convergencia y divergencia en los controles de seguridad propuestos para la tecnología de nube.

- Basándose en las buenas prácticas identificadas y la comparativa de marcos de referencia, se desarrolló la propuesta de controles de seguridad para la tecnología de nube. Estos controles abarcan aspectos fundamentales de la seguridad, como la gestión de identidades y accesos, la protección de datos en tránsito y en reposo, la evaluación continua y la implementación de políticas de seguridad.

- La elección entre el Marco de Ciberseguridad del NIST, NIST 800-53, ISO 27001 entre otras, dependerá de las necesidades y objetivos de cada organización, así como regulaciones o estándares que deban cumplir según su ámbito de competencia.

RECOMENDACIONES

- Implementar controles de seguridad, basados en la integración de estándares, marcos de referencia y buenas prácticas empleadas por proveedores de servicios en la nube, que permitirá fortalecer la seguridad en la nube y garantizar una protección sólida para los datos y recursos de la organización.

- Mantener una revisión continua de los controles de seguridad implementados, en función de las nuevas amenazas y tendencias en la seguridad en la nube, de forma que las organizaciones puedan actuar de manera proactiva ante cualquier evento de seguridad informática.

- Capacitar y concientizar al personal de la organización en la importancia de la implementación y uso efectivo de los controles de seguridad en la nube, contribuirá significativamente a la mitigación de riesgos y a una respuesta adecuada ante incidentes de seguridad.

- Fomentar la colaboración entre proveedores de servicios en la nube y promover la cooperación entre países, a través del intercambio de experiencias e información en materia de seguridad, esto contribuirá con la adopción de leyes entre naciones, fortalecerá la protección de varios tipos de servicios en internet y ayudará a combatir de manera efectiva los delitos informáticos.

BIBLIOGRAFÍA

Amazon Web Services, AWS. (2019). *¿Qué es el almacenamiento en la nube?* https://aws.amazon.com/es/what-is/cloud-storage/

Acceleration Economy. (2023). *Cloud Wars Top 10.* https://accelerationeconomy.com/cloud-wars-top-10/

Cisco Campus Technology Whitpaper. (s.f.). *Computación en la nube para la educación superior: Guía de evaluación y adopción.* https://www.cisco.com/c/dam/global/es_mx/solutions/strategy/education/connection/pdf

Corporación Internacional de Datos – IDC. (2022, junio 29). *Worldwide Public Cloud Services Revenues Grew 29.0% to $408.6 Billion in 2021.* https://www.idc.com/getdoc.jsp?containerId=prUS49420022

Corporación Internacional de Datos – IDC. (2022, feb 24). *Cloud crecerá un 30,4% en Latinoamérica para el 2023.* IDC: The premier global market intelligence company. https://www.idc.com/getdoc.jsp?containerId=prLA49041222

European Network and Information Security Agency. Europa.eu. (2022), *Beneficios, riesgos y recomendaciones para la seguridad de la información.* https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Evaluando Cloud. (2018, abril 9). *Seguridad y privacidad en la nube ¿de quién es la responsabilidad?* https://evaluandocloud.com/seguridad-privacidad-la-nube-quien-la-responsabilidad/

FireEye. (2021). Cyber Security Predictions 2021 https://vpnoverview.com/wp-content/uploads/fire-eye-rpt-security-predictions-2021-1.pdf

Schulze, H., Fortinet.com. (2022). *Cloud Security Report 2022* https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-cloud-security.pdf

Internal Revenue Service – IRS. (2022, August 29). *Cloud computing environment*. from https://www.irs.gov/privacy-disclosure/cloud-computing-environment

Kaspersky. (2023, abril 19). *¿Qué es la seguridad en la nube?* https://latam.kaspersky.com/resource-center/definitions/what-is-cloud-security

Kaspersky. (2023, abril 19). *Problemas y riesgos de la seguridad en la nube.* https://latam.kaspersky.com/resource-center/preemptive-safety/cloud-security-issues-challenges

Mell, P. M., & Grance, T. (2011). *The NIST definition of cloud computing.* National Institute of Standards and Technology.

NIST. (2018). *Cybersecurity Framework Components.* https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components

Organización Internacional de Normalización. (2013). *ISO 27001*. Obtenido de iso.org https://www.iso.org/isoiec-27001-information-security.html

Ramírez, J. C., Luque, L. C., & Olivares, J. G. (2017). *Introducción a la seguridad en cloud computing*.

Stine, K., & Barrett, M. National Institute of Standards and Technology. (2022). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* https://doi.org/10.6028/NIST.CSWP.04162018es

S. Potluri, K. Subba Rao & S. Nandan Mohanty (Ed.). (2021). *Techniques and Applications (Vol. 1) [Libro electrónico]. De Gruyter.* https://doi.org/10.1515/9783110732573-202

Thalesgroup.com. (2021). *Estudio de Thales sobre seguridad en la nube de 2021* https://cpl.thalesgroup.com/2021/euro-cloud-security-research

UNIVERSIDAD TECNOLÓGICA ISRAEL. Edu.ec. (2022). *Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS* https://repositorio.uisrael.edu.ec/bitstream/47000/3365/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-008.pdf

Vera-Cruz, C. (2021, mayo 27). *Empresas en la nube: Oportunidades y riesgos que se deben considerar.* ComputerWeekly.es; TechTarget. https://www.computerweekly.com/es/cronica/Empresas-en-la-nube-Oportunidades-y-riesgos-que-se-deben-considerar

ANEXOS

Detalles de la iniciativa integrada del cumplimiento normativo de NIST SP 800-53 Rev. 4

Artículo • 18/04/2023

En el artículo siguiente se detalla la correspondencia entre los **dominios de cumplimiento** y los **controles** de la definición de la iniciativa integrada del cumplimiento normativo de Azure Policy y NIST SP 800-53 Rev. 4. Para más información sobre este estándar de cumplimiento, consulte NIST SP 800-53 Rev. 4 . Para entender el concepto de *propiedad*, consulte Definición de directivas de Azure Policy y Responsabilidad compartida en la nube.

Las siguientes asignaciones son para los controles de **NIST SP 800-53 Rev. 4**. Muchos de los controles se implementan con una definición de iniciativa de Azure Policy. Para revisar la definición de iniciativa completa, abra **Policy** en Azure Portal y seleccione la página **Definiciones**. Después, busque y seleccione la definición de la iniciativa integrada del cumplimiento normativo de **NIST SP 800-53 Rev. 4**.

> **Importante**
>
> Cada control que se muestra a continuación está asociado a una o varias definiciones de **Azure Policy**. Estas directivas pueden ayudarle a **evaluar el cumplimiento** mediante el control. Sin embargo, con frecuencia no hay una correspondencia completa o exacta entre un control y una o varias directivas. Como tal, el **cumplimiento** en Azure Policy solo se refiere a las propias definiciones de directiva; esto no garantiza que se cumpla totalmente con todos los requisitos de un control. Además, el estándar de cumplimiento incluye controles que no se abordan con las definiciones de Azure Policy en este momento. Por lo tanto, el cumplimiento en Azure Policy es solo una vista parcial del estado general de cumplimiento. Las asociaciones entre los dominios de cumplimiento, los controles y las definiciones de Azure Policy para este estándar de cumplimiento pueden cambiar con el tiempo. Para ver el historial de cambios, consulte el **historial de confirmación de GitHub** .

Control de acceso

Procedimientos y directiva de control de acceso

Id. : NIST SP 800-53 Rev. 4 AC-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1000: directiva y procedimientos de control de acceso	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1001: directiva y procedimientos de control de acceso	Microsoft implementa este control de Access Control	auditoría	1.0.0

Administración de cuentas

Id. : NIST SP 800-53 Rev. 4 AC-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe designar un máximo de tres propietarios para la suscripción	Se recomienda que designe a un máximo de tres propietarios de suscripción para reducir el riesgo de una brecha de seguridad por parte de un propietario en peligro.	AuditIfNotExists, Disabled	3.0.0
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft		
Auditar el uso de reglas de RBAC personalizadas	Permite auditar roles integrados, como "propietario, colaborador, lector" en lugar de roles RBAC personalizados, que son propensos a errores de auditoría. El uso de roles personalizados se trata como una excepción y requiere una revisión rigurosa y el modelado de amenazas.	Audit, Disabled	1.0.0
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.	Audit, Deny, Disabled	1.0.0
Las cuentas en desuso deben quitarse de la suscripción	Convendría eliminar las cuentas en desuso de las suscripciones. Las cuentas en desuso son cuentas en las que se ha bloqueado el inicio de sesión.	AuditIfNotExists, Disabled	3.0.0
Las cuentas en desuso con permisos de propietario deben quitarse de la suscripción	Quitar de la suscripción las cuentas en desuso con permisos de propietario Las cuentas en desuso son cuentas en las que se ha bloqueado el inicio de sesión.	AuditIfNotExists, Disabled	3.0.0
Las cuentas externas con permisos de propietario deben quitarse de la suscripción	Las cuentas externas con permisos de propietario deben quitarse de la suscripción a fin de evitar el acceso no supervisado.	AuditIfNotExists, Disabled	3.0.0
Las cuentas externas con permisos de lectura deben quitarse de la suscripción	Las cuentas externas con privilegios de lectura deben quitarse de la suscripción a fin de evitar el acceso no supervisado.	AuditIfNotExists, Disabled	3.0.0
Las cuentas externas con permisos de escritura deben quitarse de la suscripción	Las cuentas externas con privilegios de escritura deben quitarse de la suscripción a fin de evitar el acceso no supervisado.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La identidad administrada debe usarse en la aplicación de API	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación de funciones	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación web	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
Control administrado por Microsoft 1002: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1003: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1004: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1005: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1006: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1007: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1008: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1009: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1010: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1011: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1012: administración de cuentas	Microsoft implementa este control de Access Control	auditoría	1.0.0
Los clústeres de Service Fabric solo deben usar Azure Active Directory para la autenticación de cliente	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0

Administración de cuentas de sistema automatizadas

Id. : NIST SP 800-53 Rev. 4 AC-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft	AuditIfNotExists, Disabled	1.0.0
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.		
Control administrado por Microsoft 1013: administración de cuentas | Administración automatizada de cuentas del sistema	Microsoft implementa este control de Access Control	auditoría	1.0.0
Los clústeres de Service Fabric solo deben usar Azure Active Directory para la autenticación de cliente	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0

Eliminación de cuentas temporales o de emergencia

Id. : NIST SP 800-53 Rev. 4 AC-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1014: administración de cuentas | Eliminación de cuentas de emergencia y temporales	Microsoft implementa este control de Access Control	auditoría	1.0.0

Deshabilitación de cuentas inactivas

Id. : NIST SP 800-53 Rev. 4 AC-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1015: administración de cuentas | Deshabilitación de cuentas inactivas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Acciones de auditoría automatizadas

Id. : NIST SP 800-53 Rev. 4 AC-2 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1016: administración de cuentas | Acciones de auditoría automatizadas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Cierre de sesión por inactividad

Id. : NIST SP 800-53 Rev. 4 AC-2 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1017: administración de cuentas | Cierre de sesión por inactividad	Microsoft implementa este control de Access Control	auditoría	1.0.0

Esquemas basados en roles

Id. : NIST SP 800-53 Rev. 4 AC-2 (7)

Nombre (Azure Portal)	**Descripción**	**Efectos**	**Versión** (GitHub)
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft	AuditIfNotExists, Disabled	1.0.0
Auditar el uso de reglas de RBAC personalizadas	Permite auditar roles integrados, como "propietario, colaborador, lector" en lugar de roles RBAC personalizados, que son propensos a errores de auditoría. El uso de roles personalizados se trata como una excepción y requiere una revisión rigurosa y el modelado de amenazas.	Audit, Disabled	1.0.0
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.	Audit, Deny, Disabled	1.0.0
Control administrado por Microsoft 1018: administración de cuentas | Esquemas basados en roles	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1019: administración de cuentas | Esquemas basados en roles	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1020: administración de cuentas | Esquemas basados en roles	Microsoft implementa este control de Access Control	auditoría	1.0.0
Los clústeres de Service Fabric solo deben usar Azure Active Directory para	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Autenticación de cliente			
Para proteger las suscripciones se deben usar entidades de servicio, en lugar de certificados de administración .	Los certificados de administración permiten a quien se autentica con ellos administrar las suscripciones a las que están asociados. Para administrar las suscripciones de forma más segura, al usar entidades de servicio con Resource Manager se recomienda limitar el impacto de un certificado si el certificado correo peligro.	AuditIfNotExists, Disabled	1.0.0

Restricciones de uso de cuentas de grupo o compartidas

Id. : NIST SP 800-53 Rev. 4 AC-2 (9)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1021: administración de cuentas | Restricciones de uso de cuentas de grupo o compartidas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Terminación de credenciales de cuentas de grupo o compartidas

Id. : NIST SP 800-53 Rev. 4 AC-2 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1022: administración de cuentas | Terminación de credenciales de cuentas de grupo o compartidas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Condiciones de uso

Id. : NIST SP 800-53 Rev. 4 AC-2 (11)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1023: administración de cuentas | Condiciones de uso	Microsoft implementa este control de Access Control	auditoría	1.0.0

Supervisión de cuentas o uso atípico

Id. : NIST SP 800-53 Rev. 4 AC-2 (12)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
SQL Server en las máquinas	amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.		
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
Los puertos de administración de las máquinas virtuales deben protegerse con el control de acceso de red Just-In-Time .	Azure Security Center supervisará el posible acceso de red Just-In-Time (JIT) como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1024: administración de cuentas | Supervisión de cuentas o uso atípico	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1025: administración de cuentas | Supervisión de cuentas o uso atípico	Microsoft implementa este control de Access Control	auditoría	1.0.0

Deshabilitación de cuentas para individuos de alto riesgo

Id. : NIST SP 800-53 Rev. 4 AC-2 (13)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1026: administración de cuentas | Deshabilitación de cuentas para individuos de alto riesgo	Microsoft implementa este control de Access Control	auditoría	1.0.0

Aplicación de acceso

Id. : NIST SP 800-53 Rev. 4 AC-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales sin identidades	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado pero no tienen identidades administradas. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado y que tienen al menos una identidad asignada por el usuario, pero no tienen ninguna identidad administrada asignada por el sistema. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de	modify	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
con una identidad asignada por el usuario	usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.		
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Linux que tengan cuentas sin contraseña	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Linux tienen cuentas sin contraseña.	AuditIfNotExists, Disabled	1.0.0
La autenticación en máquinas Linux debe requerir claves SSH.	Aunque el propio SSH proporciona una conexión cifrada, el uso de contraseñas con SSH deja la máquina virtual vulnerable a ataques por fuerza bruta. La opción más segura para autenticarse en una máquina virtual Linux de Azure mediante SSH es con un par de claves pública y privada, también conocido como claves SSH. Más información: https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed.	AuditIfNotExists, Disabled	2.0.1
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.	Audit, Deny, Disabled	1.0.0
Implementar la extensión de configuración de invitado de Linux para permitir las asignaciones de configuración de invitado en máquinas virtuales Linux	Esta directiva implementa la extensión de configuración de invitado de Linux en las máquinas virtuales Linux hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Linux es un requisito previo para todas las asignaciones de configuración de invitado de Linux y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Linux. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La identidad administrada debe usarse en la aplicación de API	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación de funciones	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación web	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
MFA debe estar habilitado en las cuentas con permisos de escritura de la suscripción.	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de escritura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
MFA debe estar habilitada en las cuentas con permisos de propietario en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de propietario, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
MFA debe estar habilitada en las cuentas con permisos de lectura en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de lectura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1027: aplicación de acceso	Microsoft implementa este control de Access Control	auditoría	1.0.0
Los clústeres de Service Fabric solo deben usar Azure Active Directory para la autenticación de cliente	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se deben migrar las cuentas de almacenamiento a los nuevos recursos de Azure Resource Manager	Use el nuevo Azure Resource Manager para las cuentas de almacenamiento a fin de proporcionar mejoras de seguridad como las siguientes: mayor control de acceso (RBAC), mejor auditoría, gobernanza e implementación basados en Azure Resource Manager, acceso a las identidades administradas, acceso a los secretos de Key Vault, autenticación basada en Azure AD y compatibilidad con las etiquetas y los grupos de recursos para facilitar la administración de seguridad.	Audit, Deny, Disabled	1.0.0
Se deben migrar las máquinas virtuales a nuevos recursos de Azure Resource Manager	Use el nuevo Azure Resource Manager para las máquinas virtuales a fin de proporcionar mejoras de seguridad como las siguientes: mayor control de acceso (RBAC), mejor auditoría, gobernanza e implementación basados en Azure Resource Manager, acceso a identidades administradas, acceso a secretos de Key Vault, autenticación basada en Azure AD y compatibilidad con etiquetas y grupos de recursos para facilitar la administración de seguridad.	Audit, Deny, Disabled	1.0.0

Control de acceso basado en rol

Id. : NIST SP 800-53 Rev. 4 AC-3 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe usar el control de acceso basado en rol (RBAC) en los servicios de Kubernetes	Para proporcionar un filtrado detallado de las acciones que los usuarios pueden realizar, use el control de acceso basado en rol (RBAC) para administrar los permisos en los clústeres de Kubernetes Service y configurar las directivas de autorización correspondientes.	Audit, Disabled	1.0.2

Aplicación del flujo de información

Id. : NIST SP 800-53 Rev. 4 AC-4

Nombre (Azure Portal)	**Descripción**	**Efectos**	**Versión** (GitHub)
Las recomendaciones de protección de red adaptable se deben aplicar en las máquinas virtuales accesibles desde Internet	Azure Security Center analiza los patrones de tráfico de máquinas virtuales orientadas a Internet y proporciona recomendaciones de reglas de grupo de seguridad de red que reducen la superficie de ataque potencial.	AuditIfNotExists, Disabled	3.0.0
Todo el tráfico de Internet debe enrutarse mediante la instancia de Azure Firewall implementada	Azure Security Center ha identificado que algunas de las subredes no están protegidas con un firewall de próxima generación. Proteja las subredes frente a posibles amenazas mediante la restricción del acceso a ellas con Azure Firewall o un firewall de próxima generación compatible.	AuditIfNotExists, Disabled	3.0.0-preview
Todos los puertos de red deben estar restringidos en los grupos de seguridad de red asociados a la máquina virtual	Azure Security Center identificó que algunas de las reglas de entrada de sus grupos de seguridad de red son demasiado permisivas. Las reglas de entrada no deben permitir el acceso desde los intervalos "Cualquiera" o "Internet". Esto podría permitir que los atacantes pudieran acceder a sus recursos.	AuditIfNotExists, Disabled	3.0.0
Los servicios de API Management deben usar una red virtual	La implementación de Azure Virtual Network ofrece una seguridad y aislamiento mejorados, y permite colocar el servicio de API Management en una red enrutable sin conexión a Internet cuyo acceso puede controlar. Estas redes se pueden conectar a las redes locales mediante diversas tecnologías de VPN, lo que permite el acceso a los servicios de back-end dentro de la red o de forma local. El portal para desarrolladores y la puerta de enlace de API pueden configurarse para que sea accesible desde Internet o solo dentro de la red virtual.	Audit, Disabled	1.0.1
App Configuration debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a las instancias de App	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Configuration en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/appconfig/private-endpoint.		
Los intervalos IP autorizados deben definirse en los servicios de Kubernetes	Restrinja el acceso a la API de administración de servicios de Kubernetes mediante la concesión de acceso de API solo a direcciones IP en intervalos específicos. Se recomienda limitar el acceso a los intervalos IP autorizados para garantizar que solo las aplicaciones de las redes permitidas puedan acceder al clúster.	Audit, Disabled	2.0.1
Azure API for FHIR debe usar un vínculo privado.	Azure API for FHIR debe tener al menos una conexión de punto de conexión privado aprobada. Los clientes de una red virtual pueden acceder de forma segura a los recursos que tengan conexiones de punto de conexión privadas mediante vínculos privados. Para más información, visite https://aka.ms/fhir-privatelink.	Audit, Disabled	1.0.0
Azure Cache for Redis debe usar Private Link	Los puntos de conexión privados le permiten conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. Al asignar puntos de conexión privados a las instancias de Azure Cache for Redis, se reduce el riesgo de pérdida de datos. Más información en: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link.	AuditIfNotExists, Disabled	1.0.0
El servicio Azure Cognitive Search debe usar una SKU que admita Private Link	Con las SKU admitidas de Azure Cognitive Search, Azure Private Link permite conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su servicio Search, se reduce el riesgo de pérdida de datos. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben deshabilitar el acceso a la red pública	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que se garantiza que el servicio de Azure Cognitive Search no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición del servicio Search. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los servicios de Azure Cognitive Search deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Cognitive Search, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Disabled	1.0.0
Las cuentas de Azure Cosmos DB deben tener reglas de firewall .	Se deben definir reglas de firewall en las cuentas de Azure Cosmos DB para evitar el tráfico desde orígenes no autorizados. Las cuentas que tienen al menos una regla de IP definida con el filtro de red virtual habilitado se consideran compatibles. Las cuentas que deshabilitan el acceso público también se consideran compatibles.	Audit, Deny, Disabled	2.0.0
Azure Data Factory debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Data Factory, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/data-factory/data-factory-private-link.	AuditIfNotExists, Disabled	1.0.0
Los dominios de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al dominio de Event Grid en lugar de a todo el servicio, también estará protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Los temas de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al tema de Event Grid en lugar	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	de a todo el servicio, estará además protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.		
Azure File Sync debe usar Private Link	Si crea un punto de conexión privado para el recurso del servicio de sincronización de almacenamiento indicado, podrá dirigirse al recurso del servicio de sincronización de almacenamiento desde el espacio de direcciones IP privadas de la red de la organización, en lugar de hacerlo a través del punto de conexión público accesible desde Internet. La creación de un punto de conexión privado por sí mismo no deshabilita el punto de conexión público.	AuditIfNotExists, Disabled	1.0.0
Azure Key Vault debe deshabilitar el acceso de red público.	Deshabilite el acceso de red público para el almacén de claves de modo que no sea accesible mediante la red pública de Internet. Esto puede reducir los riesgos de pérdida de datos. Más información en: https://aka.ms/akvprivatelink.	Audit, Deny, Disabled	2.0.0-preview
Las áreas de trabajo de Azure Machine Learning deben usar un vínculo privado .	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a áreas de trabajo de Azure Machine Learning, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link.	Audit, Deny, Disabled	1.1.0
Los espacios de nombres de Azure Service Bus deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres de Service Bus, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/service-bus-messaging/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Azure SignalR Service debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure.	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Mediante la asignación de puntos de conexión privados a su recurso de Azure SignalR Service en lugar todo el servicio, reducirá los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/asrs/privatelink.		
Las áreas de trabajo de Azure Synapse deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al área de trabajo de Azure Synapse, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links.	Audit, Disabled	1.0.1
El servicio Azure Web PubSub debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su servicio Azure Web PubSub, puede reducir los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/awps/privatelink .	Audit, Deny, Disabled	1.0.0
Las cuentas de Cognitive Services deben deshabilitar el acceso a la red pública.	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que la cuenta de Cognitive Services no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición de la cuenta de Cognitive Services. Más información en: https://go.microsoft.com/fwlink/?linkid=2129800.	Audit, Deny, Disabled	2.0.0
Las cuentas de Cognitive Services deben restringir el acceso a la red	Se debe restringir el acceso de red a las cuentas de Cognitive Services. Configure reglas de red, de forma que solo las aplicaciones de redes permitidas pueden acceder a la cuenta de Cognitive Services. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	2.0.0
Cognitive Services debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la	Audit, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a Cognitive Services, reducirá la posibilidad de pérdida de datos. Más información sobre los vínculos privados en https://go.microsoft.com/fwlink/?linkid=2129800.		
Las instancias de Container Registry no deben permitir el acceso de red sin restricciones	De manera predeterminada, las instancias de Azure Container Registry aceptan conexiones a través de Internet de hosts de cualquier red. Para protegerlas frente a posibles amenazas, permita el acceso solo desde direcciones IP públicas específicas o intervalos de direcciones. Si el registro no tiene una regla de IP/firewall o una red virtual configurada, aparece en los recursos incorrectos. Obtenga más información sobre las reglas de red de Container Registry aquí: https://aka.ms/acr/portal/public-network y aquí https://aka.ms/acr/vnet.	Audit, Deny, Disabled	1.1.0
Las instancias de Container Registry deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link controla la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a las instancias de Container Registry en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/acr/private-link.	Audit, Disabled	1.0.1
Recomendación de que CORS no permita que todos los recursos accedan a las aplicaciones web	El uso compartido de recursos entre orígenes (CORS) no debe permitir que todos los dominios accedan a la aplicación web. Permita la interacción con la aplicación web solo de los dominios requeridos.	AuditIfNotExists, Disabled	1.0.0
Las cuentas de CosmosDB deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de CosmosDB, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints.	Audit, Disabled	1.0.0
Los recursos de acceso al disco deben usar un	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
vínculo privado	conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a diskAccesses, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/disksprivatelinksdoc.		
Los espacios de nombres del centro de eventos deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres del centro de eventos, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/event-hubs/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Las máquinas virtuales accesibles desde Internet deben estar protegidas con grupos de seguridad de red	Proteja sus máquinas virtuales de posibles amenazas limitando el acceso a ellas con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0
Las instancias del servicio de aprovisionamiento de dispositivos de IoT Hub deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al servicio de aprovisionamiento de dispositivos de IoT Hub, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/iotdpsvnet.	Audit, Disabled	1.0.0
El reenvío de IP en la máquina virtual debe estar deshabilitado	Habilitar el reenvío de IP en la NIC de la máquina virtual permite que la máquina reciba tráfico dirigido a otros destinos. El reenvío de IP rara vez es necesario (por ejemplo, cuando se usa la máquina virtual como una aplicación virtual de red) y, por lo tanto, el equipo de seguridad de red debe revisarlo.	AuditIfNotExists, Disabled	3.0.0
Los puertos de administración de las	Azure Security Center supervisará el posible acceso de red Just-In-Time (JIT) como recomendaciones.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
máquinas virtuales deben protegerse con el control de acceso de red Just-In-Time .			
Se deben cerrar los puertos de administración en las máquinas virtuales	Los puertos de administración remota abiertos exponen la máquina virtual a un alto nivel de riesgo de recibir ataques basados en Internet. Estos ataques intentan averiguar las credenciales por medio de fuerza bruta a fin de obtener acceso de administrador a la máquina	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1028: aplicación del flujo de información	Microsoft implementa este control de Access Control	auditoría	1.0.0
Las máquinas virtuales sin conexión a Internet deben protegerse con grupos de seguridad de red	Proteja las máquinas virtuales no accesibles desde Internet de posibles amenazas limitando el acceso con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0
Las conexiones de punto de conexión privado en Azure SQL Database deben estar habilitadas	Las conexiones de punto de conexión privado garantizan una comunicación segura al habilitar la conectividad privada con Azure SQL Database.	Audit, Disabled	1.1.0
Se debe configurar un punto de conexión privado para Key Vault	Private Link proporciona una manera de conectar Key Vault a los recursos de Azure sin enviar tráfico a través de la red pública de Internet. Un vínculo privado proporciona varios niveles de protección contra la filtración de datos.	Audit, Deny, Disabled	1.1.0-preview
El punto de conexión privado debe estar habilitado para servidores MariaDB	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for MariaDB. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El punto de conexión privado debe estar habilitado para servidores MySQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada a Azure Database for MySQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores PostgreSQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for PostgreSQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
Debe deshabilitarse el acceso a redes públicas en Azure SQL Database	Al deshabilitar la propiedad de acceso a la red pública, se mejora la seguridad al garantizar que solo se pueda acceder a la instancia de Azure SQL Database desde un punto de conexión privado. Esta configuración deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o redes virtuales.	Audit, Deny, Disabled	1.1.0
El acceso a redes públicas debe estar deshabilitado para los servidores MariaDB	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MariaDB desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2
El acceso a las redes públicas debe estar deshabilitado para los servidores MySQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MySQL desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El acceso a redes públicas debe estar deshabilitado para los servidores PostgreSQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for PostgreSQL desde un punto de conexión privado. Esta configuración deshabilita el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coinciden con las reglas de firewall basadas en la IP o en la red virtual.	Audit, Disabled	1.0.2
No se debe permitir el acceso público a la cuenta de almacenamiento	El acceso de lectura público anónimo a contenedores y blobs de Azure Storage es una manera cómoda de compartir datos, pero también puede plantear riesgos para la seguridad. Para evitar las infracciones de datos producidas por el acceso anónimo no deseado, Microsoft recomienda impedir el acceso público a una cuenta de almacenamiento a menos que su escenario lo requiera.	deshabilitado	3.0.1-preview
Se debe restringir el acceso de red a las cuentas de almacenamiento	El acceso de red a las cuentas de almacenamiento debe estar restringido. Configure reglas de red, solo las aplicaciones de redes permitidas pueden acceder a la cuenta de almacenamiento. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	1.1.1
Las cuentas de almacenamiento deben restringir el acceso a la red mediante el uso de reglas de red virtual	Proteja las cuentas de almacenamiento frente a amenazas potenciales mediante reglas de red virtual como método preferente en lugar de filtrado basado en IP. La deshabilitación del filtrado basado en IP evita que las direcciones IP públicas accedan a las cuentas de almacenamiento.	Audit, Deny, Disabled	1.0.1
Las cuentas de almacenamiento deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de almacenamiento, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azureprivatelinkoverview.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las subredes deben estar asociadas con un grupo de seguridad de red.	Proteja la subred de posibles amenazas mediante la restricción del acceso con un grupo de seguridad de red (NSG). Estos grupos contienen las reglas de la lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a la subred.	AuditIfNotExists, Disabled	3.0.0
Las plantillas de VM Image Builder deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los recursos de creación del generador de imágenes de máquina virtual, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet.	Audit, Disabled, Deny	1.1.0

Control de flujo de información dinámico

Id. : NIST SP 800-53 Rev. 4 AC-4 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las recomendaciones de protección de red adaptable se deben aplicar en las máquinas virtuales accesibles desde Internet	Azure Security Center analiza los patrones de tráfico de máquinas virtuales orientadas a Internet y proporciona recomendaciones de reglas de grupo de seguridad de red que reducen la superficie de ataque potencial.	AuditIfNotExists, Disabled	3.0.0
Los puertos de administración de las máquinas virtuales deben protegerse con el control de acceso de red Just-In-Time .	Azure Security Center supervisará el posible acceso de red Just-In-Time (JIT) como recomendaciones.	AuditIfNotExists, Disabled	3.0.0

Filtros de directiva de seguridad

Id. : NIST SP 800-53 Rev. 4 AC-4 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1029: aplicación del flujo de información | Filtros de directiva de seguridad	Microsoft implementa este control de Access Control	auditoría	1.0.0

Separación física o lógica de los flujos de información

Id. : NIST SP 800-53 Rev. 4 AC-4 (21)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1030: aplicación del flujo de información | Separación física o lógica de los flujos de información	Microsoft implementa este control de Access Control	auditoría	1.0.0

Separación de obligaciones

Id. : NIST SP 800-53 Rev. 4 AC-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1031: separación de obligaciones	Microsoft implementa este control de Access Control	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1032: separación de obligaciones	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1033: separación de obligaciones	Microsoft implementa este control de Access Control	auditoría	1.0.0
Debe haber más de un propietario asignado a la suscripción	Se recomienda que designe a más de un propietario de la suscripción para tener redundancia de acceso de administrador.	AuditIfNotExists, Disabled	3.0.0

Privilegios mínimos

Id. : NIST SP 800-53 Rev. 4 AC-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe designar un máximo de tres propietarios para la suscripción	Se recomienda que designe a un máximo de tres propietarios de suscripción para reducir el riesgo de una brecha de seguridad por parte de un propietario en peligro.	AuditIfNotExists, Disabled	3.0.0
Auditar el uso de reglas de RBAC personalizadas	Permite auditar roles integrados, como "propietario, colaborador, lector" en lugar de roles RBAC personalizados, que son propensos a errores de auditoría. El uso de roles personalizados se trata como una excepción y requiere una revisión rigurosa y el modelado de amenazas.	Audit, Disabled	1.0.0
Control administrado por Microsoft 1034: privilegios mínimos	Microsoft implementa este control de Access Control	auditoría	1.0.0

Autorización del acceso a las funciones de seguridad

Id. : NIST SP 800-53 Rev. 4 AC-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1035: privilegios mínimos | Autorización del acceso a las funciones de seguridad	Microsoft implementa este control de Access Control	auditoría	1.0.0

Acceso sin privilegios para las funciones que no son de seguridad

Id. : NIST SP 800-53 Rev. 4 AC-6 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1036: privilegios mínimos | Acceso sin privilegios para las funciones que no son de seguridad	Microsoft implementa este control de Access Control	auditoría	1.0.0

Acceso de red a comandos con privilegios

Id. : NIST SP 800-53 Rev. 4 AC-6 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1037: privilegios mínimos | Acceso de red a comandos con privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Cuentas con privilegios

Id. : NIST SP 800-53 Rev. 4 AC-6 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1038: privilegios mínimos | Cuentas con privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Revisión de privilegios de usuario

Id. : NIST SP 800-53 Rev. 4 AC-6 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe designar un máximo de tres propietarios para la suscripción	Se recomienda que designe a un máximo de tres propietarios de suscripción para reducir el riesgo de una brecha de seguridad por parte de un propietario en peligro.	AuditIfNotExists, Disabled	3.0.0
Auditar el uso de reglas de RBAC personalizadas	Permite auditar roles integrados, como "propietario, colaborador, lector" en lugar de roles RBAC personalizados, que son propensos a errores de auditoría. El uso de roles personalizados se trata como una excepción y requiere una revisión rigurosa y el modelado de amenazas.	Audit, Disabled	1.0.0
Control administrado por Microsoft 1039: privilegios mínimos | Revisión de privilegios de usuario	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1040: privilegios mínimos |	Microsoft implementa este control de Access Control	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Revisión de privilegios de usuario			

Niveles de privilegios para la ejecución de código

Id. : NIST SP 800-53 Rev. 4 AC-6 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1041: privilegios mínimos | Niveles de privilegios para la ejecución de código	Microsoft implementa este control de Access Control	auditoría	1.0.0

Auditoría del uso de funciones con privilegios

Id. : NIST SP 800-53 Rev. 4 AC-6 (9)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1042: privilegios mínimos | Auditoría del uso de funciones con privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Prohibición de ejecutar funciones privilegiadas para usuarios sin privilegios

Id. : NIST SP 800-53 Rev. 4 AC-6 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1043: privilegios mínimos | Prohibición de ejecutar funciones privilegiadas para usuarios sin privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Intentos de inicio de sesión incorrectos

Id. : NIST SP 800-53 Rev. 4 AC-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1044: intentos de inicio de sesión incorrectos	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1045: intentos de inicio de sesión incorrectos	Microsoft implementa este control de Access Control	auditoría	1.0.0

Purga o borrado del dispositivo móvil

Id. : NIST SP 800-53 Rev. 4 AC-7 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1046: intentos de inicio de sesión incorrectos | Purga o borrado del dispositivo móvil	Microsoft implementa este control de Access Control	auditoría	1.0.0

Notificación de uso del sistema

Id. : NIST SP 800-53 Rev. 4 AC-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1047: notificación de uso del sistema	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1048: notificación de uso del sistema	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1049: notificación de uso del sistema	Microsoft implementa este control de Access Control	auditoría	1.0.0

Control de sesiones simultáneas

Id. : NIST SP 800-53 Rev. 4 AC-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1050: control de sesiones simultáneas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Bloqueo de sesión

Id. : NIST SP 800-53 Rev. 4 AC-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1051: bloqueo de sesión	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1052: bloqueo de sesión	Microsoft implementa este control de Access Control	auditoría	1.0.0

Pantallas de patrones ocultos

Id. : NIST SP 800-53 Rev. 4 AC-11 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1053: bloqueo de sesión | Pantallas de patrones ocultos	Microsoft implementa este control de Access Control	auditoría	1.0.0

Finalización de la sesión

Id. : NIST SP 800-53 Rev. 4 AC-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1054: finalización de la sesión	Microsoft implementa este control de Access Control	auditoría	1.0.0

Cierres de sesión iniciados por el usuario / Pantallas de mensajes

Id. : NIST SP 800-53 Rev. 4 AC-12 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1055: finalización de la sesión | Cierres de sesión iniciados por el usuario / Pantallas de mensajes	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1056: finalización de la sesión | Cierres de sesión iniciados por el usuario / Pantallas de mensajes	Microsoft implementa este control de Access Control	auditoría	1.0.0

Acciones permitidas sin identificación o autenticación

Id. : NIST SP 800-53 Rev. 4 AC-14

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1057: acciones permitidas sin identificación o autenticación	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1058: acciones permitidas sin identificación o autenticación	Microsoft implementa este control de Access Control	auditoría	1.0.0

Atributos de seguridad

Id. : NIST SP 800-53 Rev. 4 AC-16

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2

Acceso remoto

Id. : NIST SP 800-53 Rev. 4 AC-17

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales sin identidades	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado pero no tienen identidades administradas. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales con una identidad asignada por el usuario	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado y que tienen al menos una identidad asignada por el usuario, pero no tienen ninguna identidad administrada asignada por el sistema. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
App Configuration debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a las instancias de App Configuration en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/appconfig/private-endpoint.	AuditIfNotExists, Disabled	1.0.2
Auditar las máquinas Linux que permitan conexiones remotas desde cuentas sin contraseña	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Linux permiten la conexión remota de cuentas sin contraseña.	AuditIfNotExists, Disabled	1.0.0
Azure API for FHIR debe usar un vínculo privado.	Azure API for FHIR debe tener al menos una conexión de punto de conexión privado aprobada. Los clientes de una red virtual pueden acceder de forma segura a los recursos que tengan conexiones de punto de conexión privadas mediante vínculos privados. Para más información, visite https://aka.ms/fhir-privatelink.	Audit, Disabled	1.0.0
Azure Cache for Redis debe residir en una red virtual	La implementación de Azure Virtual Network proporciona seguridad y aislamiento mejorados para Azure Cache for Redis, así como subredes, directivas de control de acceso y otras características para restringir aún más el acceso. Cuando una instancia de Azure Cache for Redis está configurada con una red virtual, no está disponible públicamente y solo se puede acceder a ella desde máquinas virtuales y aplicaciones de la red virtual.	Audit, Deny, Disabled	1.0.3
Azure Cache for Redis debe usar Private Link	Los puntos de conexión privados le permiten conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. Al asignar puntos de conexión privados a las instancias de Azure Cache for Redis, se reduce el riesgo de pérdida de datos. Más información en: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El servicio Azure Cognitive Search debe usar una SKU que admita Private Link	Con las SKU admitidas de Azure Cognitive Search, Azure Private Link permite conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su servicio Search, se reduce el riesgo de pérdida de datos. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Cognitive Search, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Disabled	1.0.0
Azure Data Factory debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Data Factory, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/data-factory/data-factory-private-link.	AuditIfNotExists, Disabled	1.0.0
Los dominios de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al dominio de Event Grid en lugar de a todo el servicio, también estará protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los temas de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al tema de Event Grid en lugar de a todo el servicio, estará además protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Azure File Sync debe usar Private Link	Si crea un punto de conexión privado para el recurso del servicio de sincronización de almacenamiento indicado, podrá dirigirse al recurso del servicio de sincronización de almacenamiento desde el espacio de direcciones IP privadas de la red de la organización, en lugar de hacerlo a través del punto de conexión público accesible desde Internet. La creación de un punto de conexión privado por sí mismo no deshabilita el punto de conexión público.	AuditIfNotExists, Disabled	1.0.0
Las áreas de trabajo de Azure Machine Learning deben usar un vínculo privado .	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a áreas de trabajo de Azure Machine Learning, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link.	Audit, Deny, Disabled	1.1.0
Los espacios de nombres de Azure Service Bus deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres de Service Bus, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/service-bus-messaging/private-link-service.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure SignalR Service debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su recurso de Azure SignalR Service en lugar todo el servicio, reducirá los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/asrs/privatelink.	Audit, Deny, Disabled	1.0.1
Azure Spring Cloud debe usar la inserción de red	Las instancias de Azure Spring Cloud deberían utilizar la inserción de red virtual con los fines siguientes: 1. Aislar Azure Spring Cloud de Internet. 2. Permitir que Azure Spring Cloud interactúe con sistemas en centros de datos locales o con el servicio de Azure en otras redes virtuales. 3. Permite a los clientes controlar las comunicaciones de red entrantes y salientes para Azure Spring Cloud.	Audit, Disabled, Deny	1.0.0
Las áreas de trabajo de Azure Synapse deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al área de trabajo de Azure Synapse, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links.	Audit, Disabled	1.0.1
El servicio Azure Web PubSub debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su servicio Azure Web PubSub, puede reducir los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/awps/privatelink .	Audit, Deny, Disabled	1.0.0
Cognitive Services debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link	Audit, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a Cognitive Services, reducirá la posibilidad de pérdida de datos. Más información sobre los vínculos privados en https://go.microsoft.com/fwlink/?linkid=2129800.		
Las instancias de Container Registry deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link controla la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a las instancias de Container Registry en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/acr/private-link.	Audit, Disabled	1.0.1
Las cuentas de CosmosDB deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de CosmosDB, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints.	Audit, Disabled	1.0.0
Implementar la extensión de configuración de invitado de Linux para permitir las asignaciones de configuración de invitado en máquinas virtuales Linux	Esta directiva implementa la extensión de configuración de invitado de Linux en las máquinas virtuales Linux hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Linux es un requisito previo para todas las asignaciones de configuración de invitado de Linux y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Linux. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Implementar la extensión de configuración de invitado de Windows para permitir las asignaciones de configuración	Esta directiva implementa la extensión de configuración de invitado de Windows en las máquinas virtuales Windows hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Windows es un requisito previo para todas las asignaciones de configuración de invitado de Windows y debe implementarse en las máquinas antes de usar cualquier definición	deployIfNotExists	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
de invitado en máquinas virtuales Windows	de directiva de configuración de invitado de Windows. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.		
Los recursos de acceso al disco deben usar un vínculo privado	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a diskAccesses, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/disksprivatelinksdoc.	AuditIfNotExists, Disabled	1.0.0
Los espacios de nombres del centro de eventos deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres del centro de eventos, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/event-hubs/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Las instancias del servicio de aprovisionamiento de dispositivos de IoT Hub deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al servicio de aprovisionamiento de dispositivos de IoT Hub, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/iotdpsvnet.	Audit, Disabled	1.0.0
Control administrado por Microsoft 1059: acceso remoto	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1060: acceso remoto	Microsoft implementa este control de Access Control	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las conexiones de punto de conexión privado en Azure SQL Database deben estar habilitadas	Las conexiones de punto de conexión privado garantizan una comunicación segura al habilitar la conectividad privada con Azure SQL Database.	Audit, Disabled	1.1.0
Se debe configurar un punto de conexión privado para Key Vault	Private Link proporciona una manera de conectar Key Vault a los recursos de Azure sin enviar tráfico a través de la red pública de Internet. Un vínculo privado proporciona varios niveles de protección contra la filtración de datos.	Audit, Deny, Disabled	1.1.0-preview
El punto de conexión privado debe estar habilitado para servidores MariaDB	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for MariaDB. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores MySQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada a Azure Database for MySQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores PostgreSQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for PostgreSQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
La depuración remota debe estar desactivada para las aplicaciones de API	La depuración remota requiere puertos de entrada que se abran en una aplicación de API. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La depuración remota debe estar desactivada para las aplicaciones de funciones	La depuración remota requiere puertos de entrada que se abran en una instancia de aplicaciones de funciones. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
Recomendación de desactivación de la depuración remota para aplicaciones web	La depuración remota requiere puertos de entrada que se abran en una aplicación web. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
Se debe restringir el acceso de red a las cuentas de almacenamiento	El acceso de red a las cuentas de almacenamiento debe estar restringido. Configure reglas de red, solo las aplicaciones de redes permitidas pueden acceder a la cuenta de almacenamiento. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	1.1.1
Las cuentas de almacenamiento deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de almacenamiento, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azureprivatelinkoverview.	AuditIfNotExists, Disabled	2.0.0
Las plantillas de VM Image Builder deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los recursos de creación del generador de imágenes de máquina virtual, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet.	Audit, Disabled, Deny	1.1.0

Supervisión y control automatizados

Id. : NIST SP 800-53 Rev. 4 AC-17 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales sin identidades	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado pero no tienen identidades administradas. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales con una identidad asignada por el usuario	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado y que tienen al menos una identidad asignada por el usuario, pero no tienen ninguna identidad administrada asignada por el sistema. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
App Configuration debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a las instancias de App Configuration en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/appconfig/private-endpoint.	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Auditar las máquinas Linux que permitan conexiones remotas desde cuentas sin contraseña	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Linux permiten la conexión remota de cuentas sin contraseña.	AuditIfNotExists, Disabled	1.0.0
Azure API for FHIR debe usar un vínculo privado.	Azure API for FHIR debe tener al menos una conexión de punto de conexión privado aprobada. Los clientes de una red virtual pueden acceder de forma segura a los recursos que tengan conexiones de punto de conexión privadas mediante vínculos privados. Para más información, visite https://aka.ms/fhir-privatelink.	Audit, Disabled	1.0.0
Azure Cache for Redis debe residir en una red virtual	La implementación de Azure Virtual Network proporciona seguridad y aislamiento mejorados para Azure Cache for Redis, así como subredes, directivas de control de acceso y otras características para restringir aún más el acceso. Cuando una instancia de Azure Cache for Redis está configurada con una red virtual, no está disponible públicamente y solo se puede acceder a ella desde máquinas virtuales y aplicaciones de la red virtual.	Audit, Deny, Disabled	1.0.3
Azure Cache for Redis debe usar Private Link	Los puntos de conexión privados le permiten conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. Al asignar puntos de conexión privados a las instancias de Azure Cache for Redis, se reduce el riesgo de pérdida de datos. Más información en: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link.	AuditIfNotExists, Disabled	1.0.0
El servicio Azure Cognitive Search debe usar una SKU que admita Private Link	Con las SKU admitidas de Azure Cognitive Search, Azure Private Link permite conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su servicio Search, se reduce el riesgo de pérdida de datos. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los servicios de Azure Cognitive Search deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Cognitive Search, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Disabled	1.0.0
Azure Data Factory debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Data Factory, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/data-factory/data-factory-private-link.	AuditIfNotExists, Disabled	1.0.0
Los dominios de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al dominio de Event Grid en lugar de a todo el servicio, también estará protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Los temas de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al tema de Event Grid en lugar de a todo el servicio, estará además protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure File Sync debe usar Private Link	Si crea un punto de conexión privado para el recurso del servicio de sincronización de almacenamiento indicado, podrá dirigirse al recurso del servicio de sincronización de almacenamiento desde el espacio de direcciones IP privadas de la red de la organización, en lugar de hacerlo a través del punto de conexión público accesible desde Internet. La creación de un punto de conexión privado por sí mismo no deshabilita el punto de conexión público.	AuditIfNotExists, Disabled	1.0.0
Las áreas de trabajo de Azure Machine Learning deben usar un vínculo privado .	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a áreas de trabajo de Azure Machine Learning, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link.	Audit, Deny, Disabled	1.1.0
Los espacios de nombres de Azure Service Bus deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres de Service Bus, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/service-bus-messaging/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Azure SignalR Service debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su recurso de Azure SignalR Service en lugar todo el servicio, reducirá los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/asrs/privatelink.	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure Spring Cloud debe usar la inserción de red	Las instancias de Azure Spring Cloud deberían utilizar la inserción de red virtual con los fines siguientes: 1. Aislar Azure Spring Cloud de Internet. 2. Permitir que Azure Spring Cloud interactúe con sistemas en centros de datos locales o con el servicio de Azure en otras redes virtuales. 3. Permite a los clientes controlar las comunicaciones de red entrantes y salientes para Azure Spring Cloud.	Audit, Disabled, Deny	1.0.0
Las áreas de trabajo de Azure Synapse deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al área de trabajo de Azure Synapse, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links.	Audit, Disabled	1.0.1
El servicio Azure Web PubSub debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su servicio Azure Web PubSub, puede reducir los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/awps/privatelink .	Audit, Deny, Disabled	1.0.0
Cognitive Services debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a Cognitive Services, reducirá la posibilidad de pérdida de datos. Más información sobre los vínculos privados en https://go.microsoft.com/fwlink/?linkid=2129800.	Audit, Disabled	2.0.0
Las instancias de Container Registry deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link controla la conectividad entre el consumidor y los servicios a través de la red troncal de Azure.	Audit, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Al asignar puntos de conexión privados a las instancias de Container Registry en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/acr/private-link.		
Las cuentas de CosmosDB deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de CosmosDB, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints.	Audit, Disabled	1.0.0
Implementar la extensión de configuración de invitado de Linux para permitir las asignaciones de configuración de invitado en máquinas virtuales Linux	Esta directiva implementa la extensión de configuración de invitado de Linux en las máquinas virtuales Linux hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Linux es un requisito previo para todas las asignaciones de configuración de invitado de Linux y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Linux. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Implementar la extensión de configuración de invitado de Windows para permitir las asignaciones de configuración de invitado en máquinas virtuales Windows	Esta directiva implementa la extensión de configuración de invitado de Windows en las máquinas virtuales Windows hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Windows es un requisito previo para todas las asignaciones de configuración de invitado de Windows y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Windows. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Los recursos de acceso al disco deben usar un vínculo privado	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a diskAccesses, se reduce el riesgo	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/disksprivatelinksdoc.		
Los espacios de nombres del centro de eventos deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres del centro de eventos, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/event-hubs/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Las instancias del servicio de aprovisionamiento de dispositivos de IoT Hub deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al servicio de aprovisionamiento de dispositivos de IoT Hub, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/iotdpsvnet.	Audit, Disabled	1.0.0
Control administrado por Microsoft 1061: acceso remoto |Supervisión o control automatizados	Microsoft implementa este control de Access Control	auditoría	1.0.0
Las conexiones de punto de conexión privado en Azure SQL Database deben estar habilitadas	Las conexiones de punto de conexión privado garantizan una comunicación segura al habilitar la conectividad privada con Azure SQL Database.	Audit, Disabled	1.1.0
Se debe configurar un punto de conexión privado para Key Vault	Private Link proporciona una manera de conectar Key Vault a los recursos de Azure sin enviar tráfico a través de la red pública de Internet. Un vínculo privado proporciona varios niveles de protección contra la filtración de datos.	Audit, Deny, Disabled	1.1.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El punto de conexión privado debe estar habilitado para servidores MariaDB	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for MariaDB. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores MySQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada a Azure Database for MySQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores PostgreSQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for PostgreSQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
La depuración remota debe estar desactivada para las aplicaciones de API	La depuración remota requiere puertos de entrada que se abran en una aplicación de API. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
La depuración remota debe estar desactivada para las aplicaciones de funciones	La depuración remota requiere puertos de entrada que se abran en una instancia de aplicaciones de funciones. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
Recomendación de desactivación de la depuración remota para aplicaciones web	La depuración remota requiere puertos de entrada que se abran en una aplicación web. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe restringir el acceso de red a las cuentas de almacenamiento	El acceso de red a las cuentas de almacenamiento debe estar restringido. Configure reglas de red, solo las aplicaciones de redes permitidas pueden acceder a la cuenta de almacenamiento. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	1.1.1
Las cuentas de almacenamiento deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de almacenamiento, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azureprivatelinkoverview.	AuditIfNotExists, Disabled	2.0.0
Las plantillas de VM Image Builder deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los recursos de creación del generador de imágenes de máquina virtual, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet.	Audit, Disabled, Deny	1.1.0

Protección de confidencialidad e integridad mediante cifrado

Id. : NIST SP 800-53 Rev. 4 AC-17 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1062: acceso remoto | Protección de confidencialidad e integridad mediante cifrado	Microsoft implementa este control de Access Control	auditoría	1.0.0

Puntos de control de acceso administrados

Id. : NIST SP 800-53 Rev. 4 AC-17 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1063: acceso remoto | Puntos de control de acceso administrados	Microsoft implementa este control de Access Control	auditoría	1.0.0

Comandos o acceso con privilegios

Id. : NIST SP 800-53 Rev. 4 AC-17 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1064: acceso remoto | Comandos o acceso con privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1065: acceso remoto | Comandos o acceso con privilegios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Desconexión o deshabilitación del acceso

Id. : NIST SP 800-53 Rev. 4 AC-17 (9)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1066: acceso remoto | Desconexión o deshabilitación del acceso	Microsoft implementa este control de Access Control	auditoría	1.0.0

Acceso inalámbrico

Id. : NIST SP 800-53 Rev. 4 AC-18

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1067: acceso inalámbrico	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1068: acceso inalámbrico	Microsoft implementa este control de Access Control	auditoría	1.0.0

Autenticación y cifrado

Id. : NIST SP 800-53 Rev. 4 AC-18 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1069: acceso inalámbrico | Autenticación y	Microsoft implementa este control de Access	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
cifrado	Control		

Deshabilitación de redes inalámbricas

Id. : NIST SP 800-53 Rev. 4 AC-18 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1070: acceso inalámbrico | Deshabilitación de redes inalámbricas	Microsoft implementa este control de Access Control	auditoría	1.0.0

Restricción de configuraciones por parte de los usuarios

Id. : NIST SP 800-53 Rev. 4 AC-18 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1071: acceso inalámbrico | Restricción de configuraciones por parte de los usuarios	Microsoft implementa este control de Access Control	auditoría	1.0.0

Niveles de potencia de las antenas y la transmisión

Id. : NIST SP 800-53 Rev. 4 AC-18 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1072: acceso inalámbrico | Niveles de potencia de las antenas y la transmisión	Microsoft implementa este control de Access Control	auditoría	1.0.0

Control de acceso para los dispositivos móviles

Id. : NIST SP 800-53 Rev. 4 AC-19

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1073: control de acceso para dispositivos móviles	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1074: control de acceso para dispositivos móviles	Microsoft implementa este control de Access Control	auditoría	1.0.0

Cifrado completo basado en contenedores o dispositivos

Id. : NIST SP 800-53 Rev. 4 AC-19 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1075: control de acceso para dispositivos móviles | Cifrado completo basado en contenedores o de dispositivos	Microsoft implementa este control de Access Control	auditoría	1.0.0

Uso de sistemas de información externos

Id. : NIST SP 800-53 Rev. 4 AC-20

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1076: uso de sistemas de información externos	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1077: uso de sistemas de información externos	Microsoft implementa este control de Access Control	auditoría	1.0.0

Límites de uso autorizado

Id. : NIST SP 800-53 Rev. 4 AC-20 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1078: uso de sistemas de información externos | Límites de uso autorizado	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1079: uso de sistemas de información externos | Límites de uso autorizado	Microsoft implementa este control de Access Control	auditoría	1.0.0

Dispositivos de almacenamiento portátiles

Id. : NIST SP 800-53 Rev. 4 AC-20 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1080: uso de sistemas de información externos | Dispositivos de almacenamiento portátiles	Microsoft implementa este control de Access Control	auditoría	1.0.0

Uso compartido de la información

Id. : NIST SP 800-53 Rev. 4 AC-21

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1081: uso compartido de la información	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1082: uso compartido de la información	Microsoft implementa este control de Access Control	auditoría	1.0.0

Contenido de acceso público

Id. : NIST SP 800-53 Rev. 4 AC-22

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1083: contenido de acceso público	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1084: contenido de acceso público	Microsoft implementa este control de Access Control	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1085: contenido de acceso público	Microsoft implementa este control de Access Control	auditoría	1.0.0
Control administrado por Microsoft 1086: contenido de acceso público	Microsoft implementa este control de Access Control	auditoría	1.0.0

Conocimiento y aprendizaje

Procedimientos y directiva de aprendizaje y reconocimiento de seguridad

Id. : NIST SP 800-53 Rev. 4 AT-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1087: procedimientos y directiva de aprendizaje y reconocimiento de seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1088: procedimientos y directiva de aprendizaje y reconocimiento de seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Aprendizaje del reconocimiento de la seguridad

Id. : NIST SP 800-53 Rev. 4 AT-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1089: aprendizaje del reconocimiento de la seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1090: aprendizaje del reconocimiento de la seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1091: aprendizaje del reconocimiento de la seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Amenaza interna

Id. : NIST SP 800-53 Rev. 4 AT-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1092: aprendizaje del reconocimiento de la seguridad | Amenaza interna	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Entrenamiento de seguridad basada en roles

Id. : NIST SP 800-53 Rev. 4 AT-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1093: aprendizaje de seguridad basada en roles	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1094: aprendizaje de seguridad basada en roles	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1095: aprendizaje de seguridad basada en roles	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Ejercicios prácticos

Id. : NIST SP 800-53 Rev. 4 AT-3 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1096: aprendizaje de seguridad basada en roles | Ejercicios prácticos	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Comunicaciones sospechosas y comportamiento anómalo del sistema

Id. : NIST SP 800-53 Rev. 4 AT-3 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1097: aprendizaje de seguridad basada en roles | Comunicaciones sospechosas y comportamiento anómalo del sistema	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Registros de aprendizaje de seguridad

Id. : NIST SP 800-53 Rev. 4 AT-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1098: registros de aprendizaje de seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0
Control administrado por Microsoft 1099: registros de aprendizaje de seguridad	Microsoft implementa este control de conocimiento y aprendizaje	auditoría	1.0.0

Auditoría y responsabilidad

Procedimientos y directivas de auditoría y rendición de cuentas

Id. : NIST SP 800-53 Rev. 4 AU-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1100: procedimientos y directivas de auditoría y rendición de cuentas	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1101: procedimientos y directivas de auditoría y rendición de cuentas	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Auditoría de eventos

Id. : NIST SP 800-53 Rev. 4 AU-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1102: eventos de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1103: eventos de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1104: eventos de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1105: eventos de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Revisiones y actualizaciones

Id. : NIST SP 800-53 Rev. 4 AU-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1106: eventos de auditoría | Revisiones y actualizaciones	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Contenido de los registros de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1107: contenido de los registros de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Información de auditoría adicional

Id. : NIST SP 800-53 Rev. 4 AU-3 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1108: contenido de los registros de auditoría | Información de auditoría adicional	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Administración centralizada del contenido de registros de auditoría planificados

Id. : NIST SP 800-53 Rev. 4 AU-3 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1109: contenido de los registros de auditoría | Administración centralizada del contenido de registros de auditoría planificados	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Capacidad de almacenamiento de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1110: auditoría de la capacidad de almacenamiento	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Respuesta a errores de procesamiento de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1111: respuesta a errores de procesamiento de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1112: respuesta a errores de procesamiento de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Capacidad de almacenamiento de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1113: respuesta a errores de procesamiento de auditoría | Capacidad de almacenamiento de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Alertas en tiempo real

Id. : NIST SP 800-53 Rev. 4 AU-5 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1114: respuesta de errores de procesamiento de auditoría | Alertas en tiempo real	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Revisión, análisis e informes de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los clústeres de Kubernetes habilitados para Azure Arc deben	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube	AuditIfNotExists, Disabled	3.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
tener la extensión de Azure Defender instalada.	para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.		
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1115: revisión, análisis e informes de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1116: revisión, análisis e informes de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe instalarse en las máquinas virtuales Windows .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0

Integración de procesos

Id. : NIST SP 800-53 Rev. 4 AU-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1117: revisión, análisis e informes de auditoría | Integración de procesos	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Correlación de repositorios de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-6 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1118: revisión, análisis e informes de auditoría | Correlación de repositorios de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Revisión y análisis centralizados

Id. : NIST SP 800-53 Rev. 4 AU-6 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La auditoría de SQL Server debe estar habilitada	La auditoría debe estar habilitada en SQL Server para realizar un seguimiento de las actividades de todas las bases de datos del servidor y guardarlas en un registro de auditoría.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El aprovisionamiento automático del agente de Log Analytics debe estar habilitado en la suscripción	A fin de supervisar las amenazas y vulnerabilidades de seguridad, Azure Security Center recopila datos de las máquinas virtuales de Azure. El agente de Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA), recopila los datos al leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copiar los datos en el área de trabajo de Log Analytics para analizarlos. Se recomienda habilitar el aprovisionamiento automático para implementar automáticamente el agente en todas las máquinas virtuales de Azure admitidas y en las nuevas que se creen.	AuditIfNotExists, Disabled	1.0.1
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La extensión "Configuración de invitado" debe estar instalada en las máquinas.	Para garantizar la seguridad de la configuración de invitado, instale la extensión "Configuración de invitado". La configuración de invitado supervisada en la extensión engloba la configuración del sistema operativo, la configuración o presencia de las aplicaciones y la configuración del entorno. Una vez instaladas, las directivas de invitado estarán disponibles como "La protección contra vulnerabilidades de Windows debe estar habilitada.". Obtenga más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1
Los problemas de estado del agente de Log Analytics se deben resolver en sus máquinas	Security Center usa el agente de Log Analytics, que anteriormente se denominaba Microsoft Monitoring Agent (MMA). Para tener la certeza de que las máquinas virtuales tienen la supervisión correcta, es preciso asegurarse de que el agente está instalado en ellas y de que recopila adecuadamente los eventos de seguridad en el área de trabajo configurada.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Linux de Azure Arc	Esta directiva audita las máquinas Linux de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El agente de Log Analytics debe instalarse en la máquina virtual para la supervisión de Azure Security Center .	Esta directiva audita cualquier máquina virtual Windows o Linux si el agente de Log Analytics no está instalado y Security Center la utiliza para supervisar las amenazas y vulnerabilidades de seguridad	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe instalarse en sus conjuntos de escalado de máquinas virtuales para supervisar Azure Security Center .	Security Center recopila datos de las máquinas virtuales de Azure para supervisar las amenazas y vulnerabilidades de la seguridad.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Windows de Azure Arc	Esta directiva audita las máquinas Windows de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
Control administrado por Microsoft 1119: revisión, análisis e informes de auditoría | Revisión y análisis centralizados	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas	AuditIfNotExists, Disabled	1.0.1-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
instalarse en las máquinas virtuales Windows .	de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.		
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0
Los registros de recursos de Azure Data Lake Store deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Azure Stream Analytics deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de las cuentas de Batch deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Data Lake Analytics deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de la instancia de Event Hubs deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de IoT Hub deben estar	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de	AuditIfNotExists, Disabled	3.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
habilitados .	seguridad o riesgo para la red.		
Los registros de recursos de Key Vault deben estar habilitados	Habilitación de la auditoría de los registros de recursos. De esta forma, puede volver a crear seguimientos de actividad con fines de investigación en caso de incidentes de seguridad o riesgos para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Logic Apps deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de los servicios Search deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Service Bus deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Virtual Machine Scale Sets deben estar habilitados	Se recomienda habilitar los registros para que ese seguimiento de actividad se pueda volver a crear cuando se necesiten investigaciones en caso de incidente o riesgo.	AuditIfNotExists, Disabled	2.0.1
La extensión "Configuración de invitado" de las máquinas virtuales debe implementarse con una identidad administrada asignada por el sistema.	La extensión Configuración de invitado requiere una identidad administrada asignada por el sistema. Si las máquinas virtuales de Azure incluidas en el ámbito de esta directiva tienen instalada la extensión "Configuración de invitado" pero no tienen una identidad administrada asignada por el sistema, no cumplirán los requisitos establecidos. Más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1

Capacidades de integración o exploración y supervisión

Id. : NIST SP 800-53 Rev. 4 AU-6 (5)

Nombre (Azure Portal)	**Descripción**	**Efectos**	**Versión** (GitHub)
La auditoría de SQL Server debe estar habilitada	La auditoría debe estar habilitada en SQL Server para realizar un seguimiento de las actividades de todas las bases de datos del servidor y guardarlas en un registro de auditoría.	AuditIfNotExists, Disabled	2.0.0
El aprovisionamiento automático del agente de Log Analytics debe estar habilitado en la suscripción	A fin de supervisar las amenazas y vulnerabilidades de seguridad, Azure Security Center recopila datos de las máquinas virtuales de Azure. El agente de Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA), recopila los datos al leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copiar los datos en el área de trabajo de Log Analytics para analizarlos. Se recomienda habilitar el aprovisionamiento automático para implementar automáticamente el agente en todas las máquinas virtuales de Azure admitidas y en las nuevas que se creen.	AuditIfNotExists, Disabled	1.0.1
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
contenedor	importadas, y expone los hallazgos detallados por imagen.		
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	protección, así como alertas sobre la actividad sospechosa.		
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La extensión "Configuración de invitado" debe estar instalada en las máquinas.	Para garantizar la seguridad de la configuración de invitado, instale la extensión "Configuración de invitado". La configuración de invitado supervisada en la extensión engloba la configuración del sistema operativo, la configuración o presencia de las aplicaciones y la configuración del entorno. Una vez instaladas, las directivas de invitado estarán disponibles como "La protección contra vulnerabilidades de Windows debe estar habilitada.". Obtenga más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1
Los problemas de estado del agente de Log Analytics se deben resolver en sus máquinas	Security Center usa el agente de Log Analytics, que anteriormente se denominaba Microsoft Monitoring Agent (MMA). Para tener la certeza de que las máquinas virtuales tienen la supervisión correcta, es preciso asegurarse de que el agente está instalado en ellas y de que recopila adecuadamente los eventos de seguridad en el área de trabajo configurada.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El agente de Log Analytics debe estar instalado en las máquinas Linux de Azure Arc	Esta directiva audita las máquinas Linux de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
El agente de Log Analytics debe instalarse en la máquina virtual para la supervisión de Azure Security Center .	Esta directiva audita cualquier máquina virtual Windows o Linux si el agente de Log Analytics no está instalado y Security Center la utiliza para supervisar las amenazas y vulnerabilidades de seguridad	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe instalarse en sus conjuntos de escalado de máquinas virtuales para supervisar Azure Security Center .	Security Center recopila datos de las máquinas virtuales de Azure para supervisar las amenazas y vulnerabilidades de la seguridad.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Windows de Azure Arc	Esta directiva audita las máquinas Windows de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
Control administrado por Microsoft 1120: revisión, análisis e informes de auditoría | Funcionalidades de integración o examen y supervisión	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe instalarse en las máquinas virtuales Windows .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0
Los registros de recursos de Azure Data Lake Store deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Azure Stream Analytics deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de las cuentas de Batch deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Data Lake Analytics deben	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de	AuditIfNotExists, Disabled	5.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
estar habilitados	seguridad o riesgo para la red.		
Los registros de recursos de la instancia de Event Hubs deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de IoT Hub deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	3.0.1
Los registros de recursos de Key Vault deben estar habilitados	Habilitación de la auditoría de los registros de recursos. De esta forma, puede volver a crear seguimientos de actividad con fines de investigación en caso de incidentes de seguridad o riesgos para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Logic Apps deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de los servicios Search deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Service Bus deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Virtual Machine Scale Sets deben estar habilitados	Se recomienda habilitar los registros para que ese seguimiento de actividad se pueda volver a crear cuando se necesiten investigaciones en caso de incidente o riesgo.	AuditIfNotExists, Disabled	2.0.1
La extensión "Configuración de invitado" de las	La extensión Configuración de invitado requiere una identidad administrada asignada por el sistema. Si las máquinas virtuales de Azure incluidas en el ámbito de esta	AuditIfNotExists, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
máquinas virtuales debe implementarse con una identidad administrada asignada por el sistema.	directiva tienen instalada la extensión "Configuración de invitado" pero no tienen una identidad administrada asignada por el sistema, no cumplirán los requisitos establecidos. Más información en https://aka.ms/gcpol.		

Correlación con supervisión física

Id. : NIST SP 800-53 Rev. 4 AU-6 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1121: revisión, análisis e informes de auditoría | Correlación con supervisión física	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Acciones permitidas

Id. : NIST SP 800-53 Rev. 4 AU-6 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1122: revisión, análisis e informes de auditoría | Acciones permitidas	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Ajuste de nivel de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-6 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1123: revisión, análisis e informes de auditoría | Ajuste de nivel de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Reducción de auditoría y generación de informes

Id. : NIST SP 800-53 Rev. 4 AU-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1124: reducción de auditoría y generación de informes	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1125: reducción de auditoría y generación de informes	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Procesamiento automático

Id. : NIST SP 800-53 Rev. 4 AU-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1126: reducción de auditoría y generación de informes | Procesamiento automático	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Marcas de tiempo

Id. : NIST SP 800-53 Rev. 4 AU-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1127: marcas de tiempo	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1128: marcas de tiempo	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Sincronización con un recurso de hora autorizado

Id. : NIST SP 800-53 Rev. 4 AU-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1129: marcas de tiempo | Sincronización con un recurso de hora autorizado	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1130: marcas de tiempo | Sincronización con un recurso de hora autorizado	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Protección de la información de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1131: protección de la información de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Auditoría de copias de seguridad en sistemas o componentes físicos separados

Id. : NIST SP 800-53 Rev. 4 AU-9 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1132: protección de la información de auditoría | Auditoría de copias de seguridad en sistemas o componentes físicos separados	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Protección criptográfica

Id. : NIST SP 800-53 Rev. 4 AU-9 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1133: protección de la información de auditoría | Protección criptográfica	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Acceso de un subconjunto de usuarios con privilegios

Id. : NIST SP 800-53 Rev. 4 AU-9 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1134: protección de la información de auditoría | Acceso de un subconjunto de usuarios con privilegios	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

No rechazo

Id. : NIST SP 800-53 Rev. 4 AU-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1135: sin rechazo	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Retención de los registros de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1136: retención de los registros de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Los servidores SQL Server con auditoría en el destino de la cuenta de	Con fines de investigación de incidentes, se recomienda establecer la retención de datos de auditoría de las instancias de SQL Server en el destino	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
almacenamiento se deben configurar con una retención de 90 días o superior.	de la cuenta de almacenamiento en al menos 90 días. Confirme que cumple las reglas de retención necesarias para las regiones en las que trabaja. A veces, es necesario para cumplir con los estándares normativos.		

Generación de auditoría

Id. : NIST SP 800-53 Rev. 4 AU-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La auditoría de SQL Server debe estar habilitada	La auditoría debe estar habilitada en SQL Server para realizar un seguimiento de las actividades de todas las bases de datos del servidor y guardarlas en un registro de auditoría.	AuditIfNotExists, Disabled	2.0.0
El aprovisionamiento automático del agente de Log Analytics debe estar habilitado en la suscripción	A fin de supervisar las amenazas y vulnerabilidades de seguridad, Azure Security Center recopila datos de las máquinas virtuales de Azure. El agente de Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA), recopila los datos al leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copiar los datos en el área de trabajo de Log Analytics para analizarlos. Se recomienda habilitar el aprovisionamiento automático para implementar automáticamente el agente en todas las máquinas virtuales de Azure admitidas y en las nuevas que se creen.	AuditIfNotExists, Disabled	1.0.1
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
No mostrar	actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La extensión "Configuración de invitado" debe estar instalada en las máquinas.	Para garantizar la seguridad de la configuración de invitado, instale la extensión "Configuración de invitado". La configuración de invitado supervisada en la extensión engloba la configuración del sistema operativo, la configuración o presencia de las aplicaciones y la configuración del entorno. Una vez instaladas, las directivas de invitado estarán disponibles como "La protección contra vulnerabilidades de Windows debe estar habilitada.". Obtenga más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los problemas de estado del agente de Log Analytics se deben resolver en sus máquinas	Security Center usa el agente de Log Analytics, que anteriormente se denominaba Microsoft Monitoring Agent (MMA). Para tener la certeza de que las máquinas virtuales tienen la supervisión correcta, es preciso asegurarse de que el agente está instalado en ellas y de que recopila adecuadamente los eventos de seguridad en el área de trabajo configurada.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Linux de Azure Arc	Esta directiva audita las máquinas Linux de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
El agente de Log Analytics debe instalarse en la máquina virtual para la supervisión de Azure Security Center .	Esta directiva audita cualquier máquina virtual Windows o Linux si el agente de Log Analytics no está instalado y Security Center la utiliza para supervisar las amenazas y vulnerabilidades de seguridad	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe instalarse en sus conjuntos de escalado de máquinas virtuales para supervisar Azure Security Center .	Security Center recopila datos de las máquinas virtuales de Azure para supervisar las amenazas y vulnerabilidades de la seguridad.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Windows de Azure Arc	Esta directiva audita las máquinas Windows de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
Control administrado por Microsoft 1137: generación	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
de auditoría			
Control administrado por Microsoft 1138: generación de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
Control administrado por Microsoft 1139: generación de auditoría	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe instalarse en las máquinas virtuales Windows .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0
Los registros de recursos de Azure Data Lake Store deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los registros de recursos de Azure Stream Analytics deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de las cuentas de Batch deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Data Lake Analytics deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de la instancia de Event Hubs deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de IoT Hub deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	3.0.1
Los registros de recursos de Key Vault deben estar habilitados	Habilitación de la auditoría de los registros de recursos. De esta forma, puede volver a crear seguimientos de actividad con fines de investigación en caso de incidentes de seguridad o riesgos para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Logic Apps deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de los servicios Search deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los registros de recursos de Service Bus deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Virtual Machine Scale Sets deben estar habilitados	Se recomienda habilitar los registros para que ese seguimiento de actividad se pueda volver a crear cuando se necesiten investigaciones en caso de incidente o riesgo.	AuditIfNotExists, Disabled	2.0.1
La extensión "Configuración de invitado" de las máquinas virtuales debe implementarse con una identidad administrada asignada por el sistema.	La extensión Configuración de invitado requiere una identidad administrada asignada por el sistema. Si las máquinas virtuales de Azure incluidas en el ámbito de esta directiva tienen instalada la extensión "Configuración de invitado" pero no tienen una identidad administrada asignada por el sistema, no cumplirán los requisitos establecidos. Más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1

Registro de auditoría en todo el sistema o en correlación con el tiempo

Id. : NIST SP 800-53 Rev. 4 AU-12 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La auditoría de SQL Server debe estar habilitada	La auditoría debe estar habilitada en SQL Server para realizar un seguimiento de las actividades de todas las bases de datos del servidor y guardarlas en un registro de auditoría.	AuditIfNotExists, Disabled	2.0.0
El aprovisionamiento automático del agente de	A fin de supervisar las amenazas y vulnerabilidades de seguridad, Azure Security Center recopila datos de las máquinas virtuales de Azure. El agente de Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA), recopila los datos	AuditIfNotExists, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Log Analytics debe estar habilitado en la suscripción	al leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copiar los datos en el área de trabajo de Log Analytics para analizarlos. Se recomienda habilitar el aprovisionamiento automático para implementar automáticamente el agente en todas las máquinas virtuales de Azure admitidas y en las nuevas que se creen.		
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
instancias de Azure SQL Server desprotegidas			
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La extensión "Configuración de invitado" debe estar instalada en las máquinas.	Para garantizar la seguridad de la configuración de invitado, instale la extensión "Configuración de invitado". La configuración de invitado supervisada en la extensión engloba la configuración del sistema operativo, la configuración o presencia de las aplicaciones y la configuración del entorno. Una vez instaladas, las directivas de invitado estarán disponibles como "La protección contra vulnerabilidades de Windows debe estar habilitada.". Obtenga más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1
Los problemas de estado del agente de Log Analytics se deben resolver en sus máquinas	Security Center usa el agente de Log Analytics, que anteriormente se denominaba Microsoft Monitoring Agent (MMA). Para tener la certeza de que las máquinas virtuales tienen la supervisión correcta, es preciso asegurarse de que el agente está instalado en ellas y de que recopila adecuadamente los eventos de seguridad en el área de trabajo configurada.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Linux de Azure Arc	Esta directiva audita las máquinas Linux de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
El agente de Log Analytics debe instalarse en la máquina virtual para la	Esta directiva audita cualquier máquina virtual Windows o Linux si el agente de Log Analytics no está instalado y Security Center la utiliza para supervisar las amenazas y vulnerabilidades de seguridad	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
supervisión de Azure Security Center .			
El agente de Log Analytics debe instalarse en sus conjuntos de escalado de máquinas virtuales para supervisar Azure Security Center .	Security Center recopila datos de las máquinas virtuales de Azure para supervisar las amenazas y vulnerabilidades de la seguridad.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Windows de Azure Arc	Esta directiva audita las máquinas Windows de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
Control administrado por Microsoft 1140: generación de auditoría | Registro de auditoría de todo el sistema o en correlación con el tiempo	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe instalarse en las máquinas virtuales Windows .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0
Los registros de recursos de Azure Data Lake Store deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Azure Stream Analytics deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de las cuentas de Batch deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Data Lake Analytics deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de la instancia de Event Hubs deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de IoT Hub deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	3.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los registros de recursos de Key Vault deben estar habilitados	Habilitación de la auditoría de los registros de recursos. De esta forma, puede volver a crear seguimientos de actividad con fines de investigación en caso de incidentes de seguridad o riesgos para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Logic Apps deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de los servicios Search deben estar habilitados .	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Service Bus deben estar habilitados	Habilitación de la auditoría de los registros de recursos. Esto le permite volver a crear seguimientos de actividad con fines de investigación en caso de incidente de seguridad o riesgo para la red.	AuditIfNotExists, Disabled	5.0.0
Los registros de recursos de Virtual Machine Scale Sets deben estar habilitados	Se recomienda habilitar los registros para que ese seguimiento de actividad se pueda volver a crear cuando se necesiten investigaciones en caso de incidente o riesgo.	AuditIfNotExists, Disabled	2.0.1
La extensión "Configuración de invitado" de las máquinas virtuales debe implementarse con una identidad administrada asignada por el sistema.	La extensión Configuración de invitado requiere una identidad administrada asignada por el sistema. Si las máquinas virtuales de Azure incluidas en el ámbito de esta directiva tienen instalada la extensión "Configuración de invitado" pero no tienen una identidad administrada asignada por el sistema, no cumplirán los requisitos establecidos. Más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1

Cambios por individuos autorizados

Id. : NIST SP 800-53 Rev. 4 AU-12 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1141: generación de auditoría | Cambios por individuos autorizados	Microsoft implementa este control de auditoría y rendición de cuentas	auditoría	1.0.0

Evaluación de seguridad y autorización

Directiva y procedimientos de autorización y valoración de seguridad

Id. : NIST SP 800-53 Rev. 4 CA-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1142: directiva y procedimientos de autorización y evaluación de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1143: directiva y procedimientos de autorización y evaluación de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Valoraciones de seguridad

Id. : NIST SP 800-53 Rev. 4 CA-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1144: evaluaciones de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1145: evaluaciones de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1146: evaluaciones de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1147: evaluaciones de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Asesores independientes

Id. : NIST SP 800-53 Rev. 4 CA-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1148: evaluaciones de seguridad | Asesores independientes	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Valoraciones especializadas

Id. : NIST SP 800-53 Rev. 4 CA-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1149: evaluaciones de seguridad | Valoraciones especializadas	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Organizaciones externas

Id. : NIST SP 800-53 Rev. 4 CA-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1150: evaluaciones de seguridad | Organizaciones externas	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Interconexiones del sistema

Id. : NIST SP 800-53 Rev. 4 CA-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1151: interconexiones del sistema	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1152: interconexiones del sistema	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1153: interconexiones del sistema	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Conexiones no clasificadas del sistema de seguridad no nacional

Id. : NIST SP 800-53 Rev. 4 CA-3 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1154: interconexiones del sistema | Conexiones no clasificadas del sistema de seguridad no nacional	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Restricciones de las conexiones de sistema externo

Id. : NIST SP 800-53 Rev. 4 CA-3 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1155: interconexiones del sistema | Restricciones de las conexiones de sistema externo	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Plan de acción e hitos

Id. : NIST SP 800-53 Rev. 4 CA-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1156: plan de acción e hitos	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1157: plan de acción e hitos	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Autorización de seguridad

Id. : NIST SP 800-53 Rev. 4 CA-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1158: autorización de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1159: autorización de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1160: autorización de seguridad	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Supervisión continua

Id. : NIST SP 800-53 Rev. 4 CA-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1161: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1162: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1163: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1164: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1165: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1166: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1167: supervisión continua	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Valoración independiente

Id. : NIST SP 800-53 Rev. 4 CA-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1168: supervisión continua |	Microsoft implementa este control de evaluación de	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Valoración independiente	seguridad y autorización		

Análisis de tendencias

Id. : NIST SP 800-53 Rev. 4 CA-7 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1169: supervisión continua | Análisis de tendencias	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Pruebas de penetración

Id. : NIST SP 800-53 Rev. 4 CA-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1170: pruebas de penetración	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Agente o equipo de penetración independiente

Id. : NIST SP 800-53 Rev. 4 CA-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1171: pruebas de penetración | Agente o equipo de penetración independiente	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Conexiones internas del sistema

Id. : NIST SP 800-53 Rev. 4 CA-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1172: conexiones internas del sistema	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0
Control administrado por Microsoft 1173: conexiones internas del sistema	Microsoft implementa este control de evaluación de seguridad y autorización	auditoría	1.0.0

Administración de la configuración

Procedimientos y directivas de administración de configuración

Id. : NIST SP 800-53 Rev. 4 CM-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1174: procedimientos y directivas de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1175: procedimientos y directivas de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Configuración de línea de base

Id. : NIST SP 800-53 Rev. 4 CM-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1176: configuración de línea de base	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Revisiones y actualizaciones

Id. : NIST SP 800-53 Rev. 4 CM-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1177: configuración de línea de base | Revisiones y actualizaciones	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1178: configuración de línea de base | Revisiones y actualizaciones	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1179: configuración de línea de base | Revisiones y actualizaciones	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Compatibilidad de automatización para precisión o moneda

Id. : NIST SP 800-53 Rev. 4 CM-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1180: configuración de línea de base | Compatibilidad de automatización para precisión o moneda	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Retención de configuraciones anteriores

Id. : NIST SP 800-53 Rev. 4 CM-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1181: configuración de línea de base | Retención de configuraciones anteriores	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Configuración de sistemas, componentes o dispositivos para áreas de alto riesgo

Id. : NIST SP 800-53 Rev. 4 CM-2 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1182: configuración de línea de base | Configuración de sistemas, componentes o dispositivos para áreas de alto riesgo	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1183: configuración de línea de base | Configuración de sistemas, componentes o dispositivos para áreas de alto riesgo	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Control de cambios de configuración

Id. : NIST SP 800-53 Rev. 4 CM-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1184: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1185: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1186: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1187: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1188: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1189: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1190: control de cambios de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Documento, notificación o prohibición automáticos de cambios

Id. : NIST SP 800-53 Rev. 4 CM-3 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1191: control de cambios de configuración | Documento, notificación o prohibición automáticos de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1192: control de cambios de configuración | Documento, notificación o prohibición automáticos de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1193: control de cambios de configuración | Documento, notificación o prohibición automáticos de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1194: control de cambios de configuración |	Microsoft implementa este control de	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Documento, notificación o prohibición automáticos de cambios	administración de configuración		
Control administrado por Microsoft 1195: control de cambios de configuración | Documento, notificación o prohibición automáticos de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1196: control de cambios de configuración | Documento, notificación o prohibición automáticos de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Prueba, validación o documentación de cambios

Id. : NIST SP 800-53 Rev. 4 CM-3 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1197: control de cambios de configuración | Prueba, validación o documentación de cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Representante de seguridad

Id. : NIST SP 800-53 Rev. 4 CM-3 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1198: control de cambios de configuración | Representante de seguridad	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Administración de criptografía

Id. : NIST SP 800-53 Rev. 4 CM-3 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1199: control de cambios de configuración | Administración de criptografía	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Análisis del impacto de seguridad

Id. : NIST SP 800-53 Rev. 4 CM-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1200: análisis del impacto en la seguridad	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Separación de entornos de prueba

Id. : NIST SP 800-53 Rev. 4 CM-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1201: análisis del impacto en la seguridad | Separación de entornos de prueba	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Restricciones de acceso para cambios

Id. : NIST SP 800-53 Rev. 4 CM-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1202: restricciones de acceso para cambios	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Cumplimiento de acceso o auditoría automatizados

Id. : NIST SP 800-53 Rev. 4 CM-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1203: restricciones de acceso para cambios | Cumplimiento de acceso o auditoría automatizados	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Revisión de los cambios del sistema

Id. : NIST SP 800-53 Rev. 4 CM-5 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1204: restricciones de acceso para cambios | Revisión de los cambios del sistema	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Componentes firmados

Id. : NIST SP 800-53 Rev. 4 CM-5 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1205: restricciones de acceso para cambios | Componentes firmados	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Limitación de privilegios de producción u operativos

Id. : NIST SP 800-53 Rev. 4 CM-5 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1206: restricciones de acceso para cambios | Limitación de privilegios de producción u operativos	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1207: restricciones de acceso para cambios | Limitación de privilegios de producción u operativos	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Valores de configuración

Id. : NIST SP 800-53 Rev. 4 CM-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El complemento Azure Policy para Kubernetes Service (AKS) debería estar instalado y habilitado en sus clústeres	El complemento Azure Policy para Kubernetes Service (AKS) amplía Gatekeeper v3, un webhook del controlador de admisión de Open Policy Agent (OPA), para aplicar imposiciones y medidas de seguridad a escala en los clústeres de forma centralizada y coherente.	Audit, Disabled	1.0.2
CORS no debe permitir que todos los recursos accedan a la aplicación de API	El uso compartido de recursos entre orígenes (CORS) no debe permitir que todos los dominios accedan a la aplicación de API. Permita la interacción con API solo de los dominios requeridos.	AuditIfNotExists, Disabled	1.0.0
CORS no debe permitir que todos los recursos obtengan acceso a las aplicaciones de funciones	El uso compartido de recursos entre orígenes (CORS) no debe permitir que todos los dominios accedan a la aplicación de funciones. Permita la interacción con la aplicación de funciones solo de los dominios requeridos.	AuditIfNotExists, Disabled	1.0.0
Recomendación de que CORS no permita que todos los recursos accedan a las aplicaciones web	El uso compartido de recursos entre orígenes (CORS) no debe permitir que todos los dominios accedan a la aplicación web. Permita la interacción con la aplicación web solo de los dominios requeridos.	AuditIfNotExists, Disabled	1.0.0
Asegúrese de que la aplicación de API tenga la opción "Client Certificates (Incoming client certificates)" activada	Los certificados de cliente permiten que la aplicación solicite un certificado para las solicitudes entrantes. Solo los clientes que tienen un certificado válido podrán acceder a la aplicación.	Audit, Disabled	1.0.0
Asegúrese de que la aplicación web tenga la opción "Client Certificates (Incoming client certificates)" activada	Los certificados de cliente permiten que la aplicación solicite un certificado para las solicitudes entrantes. Solo los clientes que tienen un certificado válido podrán acceder a la aplicación.	Audit, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las aplicaciones de funciones deben tener la opción "Certificados de cliente (certificados de cliente entrantes)" habilitada	Los certificados de cliente permiten que la aplicación solicite un certificado para las solicitudes entrantes. Solo los clientes con certificados válidos pueden acceder a la aplicación.	Audit, Disabled	1.0.1
Asegurarse de que los límites de los recursos de memoria y CPU del contenedor no superan los límites especificados en el clúster de Kubernetes	Aplique límites de recursos de CPU y memoria de contenedor en un clúster de Kubernetes para evitar los ataques de agotamiento de recursos. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	7.0.0
Los contenedores del clúster de Kubernetes no deben compartir el identificador de proceso del host ni el espacio de nombres IPC del host	No permita que los contenedores de pods compartan el espacio de nombres de id. de proceso de host ni el espacio de nombres de IPC de host en un clúster de Kubernetes. Esta recomendación forma parte de las versiones 5.2.2 y 5.2.3 de CIS, diseñadas para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	3.0.1
Asegurarse de que los contenedores solo escuchan en los puertos permitidos en el clúster de Kubernetes	Restrinja los contenedores para que escuchen solo en puertos permitidos para proteger el acceso al clúster de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	6.1.1
Los contenedores de clúster de Kubernetes solo deben usar perfiles de AppArmor permitidos	Los contenedores solo deben usar perfiles de AppArmor permitidos en un clúster de Kubernetes. Esta recomendación forma parte de las directivas de seguridad de los pods, diseñadas para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en	deshabilitado	4.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.		
Los contenedores de clúster de Kubernetes solo deben usar funcionalidades permitidas	Restrinja las funcionalidades para reducir la superficie de contenedores expuesta a ataques en un clúster de Kubernetes. Esta recomendación forma parte de las versiones 5.2.8 y 5.2.9 de CIS, diseñadas para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	4.0.1
Asegurarse de que solo se admiten las imágenes de contenedor permitidas en el clúster de Kubernetes	Use imágenes de registros de confianza para reducir el riesgo de exposición del clúster de Kubernetes a vulnerabilidades desconocidas, problemas de seguridad e imágenes malintencionadas. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	7.0.0
Los contenedores del clúster de Kubernetes deben ejecutarse con un sistema de archivos raíz de solo lectura	Ejecute contenedores con un sistema de archivos raíz de solo lectura para protegerlos de los cambios en tiempo de ejecución con la incorporación de archivos binarios malintencionados a la ruta de acceso en un clúster de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	4.0.1
Los volúmenes hostPath del pod del clúster de Kubernetes solo deben usar rutas de host permitidas	Limite los montajes de volumen hostPath del pod a las rutas de acceso de host permitidas en un clúster de Kubernetes. Esta recomendación forma parte de las directivas de seguridad de los pods, diseñadas para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	4.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los contenedores y pods de clúster de Kubernetes solo deben ejecutarse con identificadores de usuario y grupo aprobados	Controle los id. de usuario, grupo principal, grupo adicional y grupo de sistema de archivos que los pods y los contenedores pueden usar para ejecutarse en un clúster de Kubernetes. Esta recomendación forma parte de las directivas de seguridad de los pods, diseñadas para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	4.0.1
Los pods del clúster de Kubernetes solo pueden usar redes de host e intervalos de puerto permitidos	Restringe el acceso de los pods a la red del host y el intervalo de puertos de host permitidos en un clúster de Kubernetes. Esta recomendación forma parte de la versión 5.2.4 de CIS, diseñada para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	4.0.1
Los servicios de clúster de Kubernetes solo deben escuchar en los puertos permitidos	Restrinja los servicios para que escuchen solo en puertos permitidos para proteger el acceso al clúster de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	6.1.1
No permitir contenedores con privilegios en el clúster de Kubernetes	No permita la creación de contenedores con privilegios en un clúster de Kubernetes. Esta recomendación forma parte de la versión 5.2.1 de CIS, diseñada para mejorar la seguridad de los entornos de Kubernetes. Esta directiva está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.	deshabilitado	7.0.0
Los clústeres de Kubernetes no deben permitir la	No permita que los contenedores se ejecuten con elevación de privilegios en la raíz en un clúster de Kubernetes. Esta recomendación forma parte de la versión 5.2.5 de CIS, diseñada para mejorar la seguridad de los entornos de Kubernetes. Esta directiva	deshabilitado	3.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
elevación de privilegios del contenedor	está disponible con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para obtener más información, vea https://aka.ms/kubepolicydoc.		
Las máquinas Linux deben cumplir los requisitos de la base de referencia de seguridad de procesos de Azure	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si la máquina no está configurada correctamente para una de las recomendaciones de la base de referencia de seguridad de procesos de Azure.	AuditIfNotExists, Disabled	1.1.1-preview
Control administrado por Microsoft 1208: opciones de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1209: opciones de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1210: opciones de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1211: opciones de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
La depuración remota debe estar desactivada para las aplicaciones de API	La depuración remota requiere puertos de entrada que se abran en una aplicación de API. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
La depuración remota debe estar desactivada para las	La depuración remota requiere puertos de entrada que se abran en una instancia de aplicaciones de funciones. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
aplicaciones de funciones			
Recomendación de desactivación de la depuración remota para aplicaciones web	La depuración remota requiere puertos de entrada que se abran en una aplicación web. Se debe desactivar la depuración remota.	AuditIfNotExists, Disabled	1.0.0
Las máquinas Windows deben cumplir los requisitos de la base de referencia de seguridad de procesos de Azure	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si la máquina no está configurada correctamente para una de las recomendaciones de la base de referencia de seguridad de procesos de Azure.	AuditIfNotExists, Disabled	1.0.1-preview

Automatización de la comprobación, la aplicación y la administración de manera centralizada

Id. : NIST SP 800-53 Rev. 4 CM-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1212: opciones de configuración Automatización de la comprobación, la aplicación y la administración de manera centralizada	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Respuesta a cambios no autorizados

Id. : NIST SP 800-53 Rev. 4 CM-6 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1213: opciones de configuración | Respuesta a cambios no autorizados	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Funcionalidad mínima

Id. : NIST SP 800-53 Rev. 4 CM-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los controles de aplicaciones adaptables para definir aplicaciones seguras deben estar habilitados en las máquinas	Habilite controles de aplicaciones para definir la lista de aplicaciones seguras conocidas que se ejecutan en las máquinas, y recibir avisos cuando se ejecuten otras aplicaciones. Esta directiva también ayuda a proteger las máquinas frente al malware. Para simplificar el proceso de configuración y mantenimiento de las reglas, Security Center usa el aprendizaje automático para analizar las aplicaciones que se ejecutan en cada máquina y sugerir la lista de aplicaciones seguras conocidas.	AuditIfNotExists, Disabled	3.0.0
Se deben actualizar las reglas de la lista de permitidos de la directiva de controles de aplicaciones adaptables	Supervise los cambios en el comportamiento de los grupos de máquinas configurados para la auditoría mediante controles de aplicaciones adaptables de Azure Security Center. Security Center usa el aprendizaje automático para analizar los procesos en ejecución en las máquinas y sugerir una lista de aplicaciones seguras conocidas. Estas se presentan como aplicaciones recomendadas que se deben permitir en directivas de control de aplicaciones adaptables.	AuditIfNotExists, Disabled	3.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1214: funcionalidad mínima	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1215: funcionalidad mínima	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Revisión periódica

Id. : NIST SP 800-53 Rev. 4 CM-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1216: funcionalidad mínima | Revisión periódica	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1217: funcionalidad mínima | Revisión periódica	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Impedimento de la ejecución del programa

Id. : NIST SP 800-53 Rev. 4 CM-7 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los controles de aplicaciones adaptables para definir aplicaciones seguras deben estar habilitados en las máquinas	Habilite controles de aplicaciones para definir la lista de aplicaciones seguras conocidas que se ejecutan en las máquinas, y recibir avisos cuando se ejecuten otras aplicaciones. Esta directiva también ayuda a proteger las máquinas frente al malware. Para simplificar el proceso de configuración y mantenimiento de las reglas, Security Center usa el aprendizaje automático para analizar las aplicaciones que se ejecutan en cada máquina y sugerir la lista de aplicaciones seguras conocidas.	AuditIfNotExists, Disabled	3.0.0
Se deben actualizar las reglas de la lista de permitidos de la directiva de controles de aplicaciones adaptables	Supervise los cambios en el comportamiento de los grupos de máquinas configurados para la auditoría mediante controles de aplicaciones adaptables de Azure Security Center. Security Center usa el aprendizaje automático para analizar los procesos en ejecución en las máquinas y sugerir una lista de aplicaciones seguras conocidas. Estas se presentan como aplicaciones recomendadas que se deben permitir en directivas de control de aplicaciones adaptables.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1218: funcionalidad mínima | Impedimento de la ejecución del programa	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Listas de permitidos y software autorizado

Id. : NIST SP 800-53 Rev. 4 CM-7 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los controles de aplicaciones adaptables para definir aplicaciones seguras deben	Habilite controles de aplicaciones para definir la lista de aplicaciones seguras conocidas que se ejecutan en las máquinas, y recibir avisos cuando se ejecuten otras aplicaciones. Esta directiva también ayuda a proteger las máquinas frente al malware.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
estar habilitados en las máquinas	Para simplificar el proceso de configuración y mantenimiento de las reglas, Security Center usa el aprendizaje automático para analizar las aplicaciones que se ejecutan en cada máquina y sugerir la lista de aplicaciones seguras conocidas.		
Se deben actualizar las reglas de la lista de permitidos de la directiva de controles de aplicaciones adaptables	Supervise los cambios en el comportamiento de los grupos de máquinas configurados para la auditoría mediante controles de aplicaciones adaptables de Azure Security Center. Security Center usa el aprendizaje automático para analizar los procesos en ejecución en las máquinas y sugerir una lista de aplicaciones seguras conocidas. Estas se presentan como aplicaciones recomendadas que se deben permitir en directivas de control de aplicaciones adaptables.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1219: funcionalidad mínima | Listas de permitidos y software autorizado	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1220: funcionalidad mínima | Listas de permitidos y software autorizado	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1221: funcionalidad mínima | Listas de permitidos y software autorizado	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Inventario de componentes del sistema de información

Id. : NIST SP 800-53 Rev. 4 CM-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1222: inventario de componentes del sistema de información	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1223: inventario de componentes del sistema de información	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Actualizaciones durante instalaciones o eliminaciones

Id. : NIST SP 800-53 Rev. 4 CM-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1224: inventario de componentes del sistema de información | Actualizaciones durante instalaciones o eliminaciones	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Mantenimiento automatizado

Id. : NIST SP 800-53 Rev. 4 CM-8 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1225: inventario de componentes del sistema de información | Mantenimiento automatizado	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Detección automatizada de componentes no autorizados

Id. : NIST SP 800-53 Rev. 4 CM-8 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1226: inventario de componentes del sistema de información | Detección automatizada de componentes no autorizados	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1227: inventario de componentes del sistema de información | Detección automatizada de componentes no autorizados	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Información de responsabilidad

Id. : NIST SP 800-53 Rev. 4 CM-8 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1228: inventario de componentes del sistema de información | Información de responsabilidad	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

No se contabilizan los componentes por duplicado

Id. : NIST SP 800-53 Rev. 4 CM-8 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1229: inventario de componentes del sistema de información | No se contabilizan los componentes por duplicado	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Plan de administración de configuración

Id. : NIST SP 800-53 Rev. 4 CM-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1230: plan de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1231: plan de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1232: plan de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1233: plan de administración de configuración	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Restricciones de uso de software

Id. : NIST SP 800-53 Rev. 4 CM-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los controles de aplicaciones adaptables para definir aplicaciones seguras deben estar habilitados en las máquinas	Habilite controles de aplicaciones para definir la lista de aplicaciones seguras conocidas que se ejecutan en las máquinas, y recibir avisos cuando se ejecuten otras aplicaciones. Esta directiva también ayuda a proteger las máquinas frente al malware. Para simplificar el proceso de configuración y mantenimiento de las reglas, Security Center usa el aprendizaje automático para analizar las aplicaciones que se ejecutan en cada máquina y sugerir la lista de aplicaciones seguras conocidas.	AuditIfNotExists, Disabled	3.0.0
Se deben actualizar las reglas de la lista de permitidos de la directiva de controles de aplicaciones adaptables	Supervise los cambios en el comportamiento de los grupos de máquinas configurados para la auditoría mediante controles de aplicaciones adaptables de Azure Security Center. Security Center usa el aprendizaje automático para analizar los procesos en ejecución en las máquinas y sugerir una lista de aplicaciones seguras conocidas. Estas se presentan como aplicaciones recomendadas que se deben permitir en directivas de control de aplicaciones adaptables.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1234: restricciones de uso de software	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1235: restricciones de uso de software	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1236: restricciones de uso de software	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Software de código abierto

Id. : NIST SP 800-53 Rev. 4 CM-10 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1237: restricciones de uso de software | Software de código abierto	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Software instalado por el usuario

Id. : NIST SP 800-53 Rev. 4 CM-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los controles de aplicaciones adaptables para definir aplicaciones seguras deben estar habilitados en las máquinas	Habilite controles de aplicaciones para definir la lista de aplicaciones seguras conocidas que se ejecutan en las máquinas, y recibir avisos cuando se ejecuten otras aplicaciones. Esta directiva también ayuda a proteger las máquinas frente al malware. Para simplificar el proceso de configuración y mantenimiento de las reglas, Security Center usa el aprendizaje automático para analizar las aplicaciones que se ejecutan en cada máquina y sugerir la lista de aplicaciones seguras conocidas.	AuditIfNotExists, Disabled	3.0.0
Se deben actualizar las reglas de la lista de permitidos de la directiva de controles de aplicaciones adaptables	Supervise los cambios en el comportamiento de los grupos de máquinas configurados para la auditoría mediante controles de aplicaciones adaptables de Azure Security Center. Security Center usa el aprendizaje automático para analizar los procesos en ejecución en las máquinas y sugerir una lista de aplicaciones seguras conocidas. Estas se presentan como aplicaciones recomendadas que se deben permitir en directivas de control de aplicaciones adaptables.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1238: software instalado por el usuario	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1239: software instalado por el usuario	Microsoft implementa este control de administración de configuración	auditoría	1.0.0
Control administrado por Microsoft 1240: software instalado por el usuario	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Alertas para instalaciones no autorizadas

Id. : NIST SP 800-53 Rev. 4 CM-11 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1241: software instalado por el usuario | Alertas para instalaciones no autorizadas	Microsoft implementa este control de administración de configuración	auditoría	1.0.0

Planes de contingencia

Procedimientos y directiva del planeamiento de contingencia

Id. : NIST SP 800-53 Rev. 4 CP-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1242: procedimientos y directiva del planeamiento de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1243: procedimientos y directiva del planeamiento de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Plan de contingencia

Id. : NIST SP 800-53 Rev. 4 CP-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1244: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1245: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1246: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1247: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1248: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1249: plan de contingencia	Microsoft implementa este control de planes de	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	contingencia		
Control administrado por Microsoft 1250: plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Coordinación con planes relacionados

Id. : NIST SP 800-53 Rev. 4 CP-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1251: plan de contingencia | Coordinación con planes relacionados	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Planificación de capacidad

Id. : NIST SP 800-53 Rev. 4 CP-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1252: plan de contingencia | Planificación de capacidad	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Reanudación de misiones esenciales o funciones empresariales

Id. : NIST SP 800-53 Rev. 4 CP-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1253: plan de contingencia | Reanudación de misiones esenciales o funciones empresariales	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Reanudación de todas las misiones o funciones empresariales

Id. : NIST SP 800-53 Rev. 4 CP-2 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1254: plan de contingencia | Reanudación de todas las misiones o funciones empresariales	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Continuación de funciones empresariales o misiones esenciales

Id. : NIST SP 800-53 Rev. 4 CP-2 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1255: plan de contingencia | Continuación de funciones empresariales o misiones esenciales	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Identificación de recursos críticos

Id. : NIST SP 800-53 Rev. 4 CP-2 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1256: plan de contingencia | Identificación de recursos críticos	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Aprendizaje sobre contingencia

Id. : NIST SP 800-53 Rev. 4 CP-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1257: aprendizaje sobre contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1258: aprendizaje sobre contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1259: aprendizaje sobre contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Eventos simulados

Id. : NIST SP 800-53 Rev. 4 CP-3 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1260: aprendizaje sobre contingencia | Eventos simulados	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Pruebas del plan de contingencia

Id. : NIST SP 800-53 Rev. 4 CP-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1261: pruebas del plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1262: pruebas del plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1263: pruebas del plan de contingencia	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Coordinación con planes relacionados

Id. : NIST SP 800-53 Rev. 4 CP-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1264: pruebas del plan de contingencia | Coordinación con planes relacionados	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Sitio de procesamiento alternativo

Id. : NIST SP 800-53 Rev. 4 CP-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1265: pruebas del plan de contingencia | Sitio de procesamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1266: pruebas del plan de contingencia | Sitio de procesamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Sitio de almacenamiento alternativo

Id. : NIST SP 800-53 Rev. 4 CP-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for MariaDB	Azure Database for MariaDB le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una	Audit, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.		
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for MySQL	Azure Database for MySQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for PostgreSQL	Azure Database for PostgreSQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
El almacenamiento con redundancia geográfica debe estar habilitado para las cuentas de almacenamiento	Use la redundancia geográfica para crear aplicaciones de alta disponibilidad.	Audit, Disabled	1.0.0
La copia de seguridad con redundancia geográfica a largo plazo debe estar habilitada para	Esta directiva audita cualquier instancia de Azure SQL Database que no tenga la copia de seguridad con redundancia geográfica habilitada.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
las instancias de Azure SQL Database			
Control administrado por Microsoft 1267: sitio de almacenamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1268: sitio de almacenamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Separación del sitio primario

Id. : NIST SP 800-53 Rev. 4 CP-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for MariaDB	Azure Database for MariaDB le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
La copia de seguridad con redundancia geográfica debe	Azure Database for MySQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro	Audit, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
estar habilitada para Azure Database for MySQL	de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.		
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for PostgreSQL	Azure Database for PostgreSQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
El almacenamiento con redundancia geográfica debe estar habilitado para las cuentas de almacenamiento	Use la redundancia geográfica para crear aplicaciones de alta disponibilidad.	Audit, Disabled	1.0.0
La copia de seguridad con redundancia geográfica a largo plazo debe estar habilitada para las instancias de Azure SQL Database	Esta directiva audita cualquier instancia de Azure SQL Database que no tenga la copia de seguridad con redundancia geográfica habilitada.	AuditIfNotExists, Disabled	2.0.0
Control administrado por Microsoft 1269: sitio de almacenamiento alternativo | Separación del sitio principal	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Objetivos de tiempo o punto de recuperación

Id. : NIST SP 800-53 Rev. 4 CP-6 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1270: sitio de almacenamiento alternativo | Objetivos de tiempo o punto de recuperación	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Accesibilidad

Id. : NIST SP 800-53 Rev. 4 CP-6 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1271: sitio de almacenamiento alternativo | Accesibilidad	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Sitio de procesamiento alternativo

Id. : NIST SP 800-53 Rev. 4 CP-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Auditoría de máquinas virtuales sin la recuperación ante desastres	Audita las máquinas virtuales que no tienen configurada la recuperación ante desastres. Para más información acerca de la recuperación ante desastres, visite	auditIfNotExists	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
configurada	https://aka.ms/asr-doc.		
Control administrado por Microsoft 1272: sitio de procesamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1273: sitio de procesamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1274: sitio de procesamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Separación del sitio primario

Id. : NIST SP 800-53 Rev. 4 CP-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1275: sitio de procesamiento alternativo | Separación del sitio principal	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Accesibilidad

Id. : NIST SP 800-53 Rev. 4 CP-7 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1276: sitio de procesamiento alternativo | Accesibilidad	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Prioridad de servicio

Id. : NIST SP 800-53 Rev. 4 CP-7 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1277: sitio de procesamiento alternativo | Prioridad de servicio	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Preparación para el uso

Id. : NIST SP 800-53 Rev. 4 CP-7 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1278: sitio de procesamiento alternativo | Preparación para el uso	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Servicios de telecomunicaciones

Id. : NIST SP 800-53 Rev. 4 CP-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1279: servicios de telecomunicaciones	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Prioridad de los aprovisionamientos de servicio

Id. : NIST SP 800-53 Rev. 4 CP-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1280: servicios de telecomunicaciones | Prioridad de los aprovisionamientos de servicio	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1281: servicios de telecomunicaciones | Prioridad de los aprovisionamientos de servicio	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Únicos puntos de error

Id. : NIST SP 800-53 Rev. 4 CP-8 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1282: servicios de telecomunicaciones | Únicos puntos de error	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Separación de proveedores principales o alternativos

Id. : NIST SP 800-53 Rev. 4 CP-8 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1283: servicios de telecomunicaciones | Separación de proveedores principales o alternativos	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Plan de contingencia del proveedor

Id. : NIST SP 800-53 Rev. 4 CP-8 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1284: servicios de telecomunicaciones | Plan de contingencia del proveedor	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1285: servicios de telecomunicaciones | Plan de contingencia del proveedor	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1286: servicios de telecomunicaciones | Plan de contingencia del proveedor	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Copia de seguridad del sistema de información

Id. : NIST SP 800-53 Rev. 4 CP-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure Backup debe estar habilitado para Virtual Machines.	Asegúrese que Azure Virtual Machines está protegido; para ello, habilite Azure Backup. Azure Backup es una solución de protección de datos segura y rentable para Azure.	AuditIfNotExists, Disabled	2.0.0
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for MariaDB	Azure Database for MariaDB le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for MySQL	Azure Database for MySQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
La copia de seguridad con redundancia geográfica debe estar habilitada para Azure Database for PostgreSQL	Azure Database for PostgreSQL le permite elegir la opción de redundancia para el servidor de bases de datos. Se puede establecer en un almacenamiento de copia de seguridad con redundancia geográfica donde los datos no solo se almacenan dentro de la región en la que se hospeda el servidor, sino que también se replican en una región emparejada para proporcionar la opción de recuperación en caso de que se produzca un error en la región. La configuración de almacenamiento con redundancia geográfica para copia de seguridad solo se permite durante la creación del servidor.	Audit, Disabled	1.0.1
Los almacenes de claves deben tener habilitada la	La eliminación malintencionada de un almacén de claves puede provocar una pérdida de datos permanente. Un usuario malintencionado de la organización puede eliminar y purgar los almacenes de claves. La protección contra purgas le protege frente a ataques	Audit, Deny, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
protección contra operaciones de purga	internos mediante la aplicación de un período de retención obligatorio para almacenes de claves eliminados temporalmente. Ningún usuario de su organización o Microsoft podrá purgar los almacenes de claves durante el período de retención de eliminación temporal.		
Los almacenes de claves deben tener habilitada la eliminación temporal	Si se elimina un almacén de claves que no tenga habilitada la eliminación temporal, se eliminarán permanentemente todos los secretos, claves y certificados almacenados en ese almacén de claves. La eliminación accidental de un almacén de claves puede provocar una pérdida de datos permanente. La eliminación temporal permite recuperar un almacén de claves eliminado accidentalmente durante un período de retención configurable.	Audit, Deny, Disabled	2.0.0
Control administrado por Microsoft 1287: copia de seguridad del sistema de información	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1288: copia de seguridad del sistema de información	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1289: copia de seguridad del sistema de información	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0
Control administrado por Microsoft 1290: copia de seguridad del sistema de información	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Pruebas de confiabilidad o integridad

Id. : NIST SP 800-53 Rev. 4 CP-9 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1291: copia de seguridad del sistema de información | Pruebas de confiabilidad o integridad	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Restauración de pruebas mediante muestreo

Id. : NIST SP 800-53 Rev. 4 CP-9 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1292: copia de seguridad del sistema de información | Restauración de pruebas mediante muestreo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Almacenamiento independiente para la información crítica

Id. : NIST SP 800-53 Rev. 4 CP-9 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1293: copia de seguridad del sistema de información | Almacenamiento independiente para la información crítica	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Transferencia al sitio de almacenamiento alternativo

Id. : NIST SP 800-53 Rev. 4 CP-9 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1294: copia de seguridad del sistema de información | Transferencia al sitio de almacenamiento alternativo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Reconstitución y recuperación del sistema de información

Id. : NIST SP 800-53 Rev. 4 CP-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1295: recuperación y reconstitución del sistema de información	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Recuperación de la transacción

Id. : NIST SP 800-53 Rev. 4 CP-10 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1296: recuperación y reconstitución del sistema de información | Recuperación de la transacción	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Restauración en el período de tiempo

Id. : NIST SP 800-53 Rev. 4 CP-10 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1297: recuperación y reconstitución del sistema de información | Restauración en el período de tiempo	Microsoft implementa este control de planes de contingencia	auditoría	1.0.0

Identificación y autenticación

Procedimientos y directivas de identificación y autenticación

Id. : NIST SP 800-53 Rev. 4 IA-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1298: procedimientos y directivas de identificación y autenticación	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1299: procedimientos y directivas de identificación y autenticación	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Identificación y autenticación (usuarios de la organización)

Id. : NIST SP 800-53 Rev. 4 IA-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft	AuditIfNotExists, Disabled	1.0.0
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.	Audit, Deny, Disabled	1.0.0
La identidad administrada debe usarse en la aplicación de API	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación de funciones	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación web	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
MFA debe estar habilitado en las cuentas con permisos de escritura de la suscripción.	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de escritura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
MFA debe estar habilitada en las cuentas con permisos de propietario en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de propietario, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
MFA debe estar habilitada en las cuentas con permisos de lectura en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de lectura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1300: identificación y autenticación (usuarios de la organización)	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Los clústeres de Service Fabric solo deben usar Azure Active Directory para la autenticación de cliente	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0
Para proteger las suscripciones se deben usar entidades de servicio, en lugar de certificados de administración .	Los certificados de administración permiten a quien se autentica con ellos administrar las suscripciones a las que están asociados. Para administrar las suscripciones de forma más segura, al usar entidades de servicio con Resource Manager se recomienda limitar el impacto de un certificado si el certificado correo peligro.	AuditIfNotExists, Disabled	1.0.0

Acceso de red a cuentas con privilegios

Id. : NIST SP 800-53 Rev. 4 IA-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
MFA debe estar habilitado en las cuentas con permisos de escritura de la suscripción.	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de escritura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
MFA debe estar habilitada en las cuentas con permisos de propietario en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	propietario, a fin de evitar una brecha de seguridad en las cuentas o los recursos.		
Control administrado por Microsoft 1301: Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso de red a cuentas sin privilegios

Id. : NIST SP 800-53 Rev. 4 IA-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
MFA debe estar habilitada en las cuentas con permisos de lectura en la suscripción	Multi-Factor Authentication (MFA) debe estar habilitada para todas las cuentas de la suscripción que tengan permisos de lectura, a fin de evitar una brecha de seguridad en las cuentas o los recursos.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1302: Identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas sin privilegios	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso local a cuentas con privilegios

Id. : NIST SP 800-53 Rev. 4 IA-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1303: Identificación y autenticación (usuarios de la organización) | Acceso local a cuentas con privilegios	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso local a cuentas sin privilegios

Id. : NIST SP 800-53 Rev. 4 IA-2 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1304: Identificación y autenticación (usuarios de la organización) | Acceso local a cuentas sin privilegios	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticación de grupos

Id. : NIST SP 800-53 Rev. 4 IA-2 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1305: identificación y autenticación (usuarios de la organización) | Autenticación de grupos	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso de red a cuentas con privilegios: resistente a reproducciones

Id. : NIST SP 800-53 Rev. 4 IA-2 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1306: identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas con privilegios: resistente a reproducciones	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso de red a cuentas sin privilegios: resistente a la reproducción

Id. : NIST SP 800-53 Rev. 4 IA-2 (9)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1307: identificación y autenticación (usuarios de la organización) | Acceso de red a cuentas sin privilegios: resistente a reproducciones	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Acceso remoto: dispositivo independiente

Id. : NIST SP 800-53 Rev. 4 IA-2 (11)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1308: identificación y autenticación (usuarios de la organización) | Acceso remoto: dispositivo independiente	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Aceptación de credenciales de PIV

Id. : NIST SP 800-53 Rev. 4 IA-2 (12)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1309: identificación y autenticación (usuarios de la organización) | Aceptación de credenciales de PIV	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Identificación y autenticación de dispositivos

Id. : NIST SP 800-53 Rev. 4 IA-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1310: identificación y autenticación de dispositivos	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Administración de identificadores

Id. : NIST SP 800-53 Rev. 4 IA-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El administrador de Azure Active Directory debe aprovisionarse para servidores SQL Server	Permite aprovisionar un administrador de Azure Active Directory para SQL Server a fin de habilitar la autenticación de Azure AD. La autenticación de Azure AD permite la administración simplificada de permisos y la administración centralizada de identidades de usuarios de base de datos y otros servicios de Microsoft	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las cuentas de Cognitive Services deben tener deshabilitados los métodos de autenticación local	La deshabilitación de métodos de autenticación local mejora la seguridad, ya que garantiza que las cuentas de Cognitive Services requieran identidades de Azure Active Directory exclusivamente para la autenticación. Más información en: https://aka.ms/cs/auth.	Audit, Deny, Disabled	1.0.0
La identidad administrada debe usarse en la aplicación de API	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación de funciones	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
La identidad administrada debe usarse en la aplicación web	Usa una identidad administrada para la seguridad de autenticación mejorada.	AuditIfNotExists, Disabled	2.0.0
Control administrado por Microsoft 1311: administración de identificadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1312: administración de identificadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1313: administración de identificadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1314: administración de identificadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1315: administración de	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
identificadores			
Los clústeres de Service Fabric solo deben usar Azure Active Directory para la autenticación de cliente	Permite auditar el uso de la autenticación de clientes solo mediante Azure Active Directory en Service Fabric	Audit, Deny, Disabled	1.1.0
Para proteger las suscripciones se deben usar entidades de servicio, en lugar de certificados de administración .	Los certificados de administración permiten a quien se autentica con ellos administrar las suscripciones a las que están asociados. Para administrar las suscripciones de forma más segura, al usar entidades de servicio con Resource Manager se recomienda limitar el impacto de un certificado si el certificado correo peligro.	AuditIfNotExists, Disabled	1.0.0

Identificación del estado del usuario

Id. : NIST SP 800-53 Rev. 4 IA-4 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1316: administración de identificadores | Identificación del estado del usuario	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Administración de autenticadores

Id. : NIST SP 800-53 Rev. 4 IA-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales sin identidades	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado pero no tienen identidades administradas. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales con una identidad asignada por el usuario	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado y que tienen al menos una identidad asignada por el usuario, pero no tienen ninguna identidad administrada asignada por el sistema. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Auditar las máquinas Linux que no tengan los permisos del archivo de contraseñas establecidos en 0644	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Linux no tienen los permisos del archivo de contraseñas establecidos en 0644.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows que no almacenen contraseñas mediante cifrado reversible	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no almacenan las contraseñas con cifrado reversible.	AuditIfNotExists, Disabled	1.0.0
La autenticación en máquinas Linux debe requerir claves SSH.	Aunque el propio SSH proporciona una conexión cifrada, el uso de contraseñas con SSH deja la máquina virtual vulnerable a ataques por fuerza bruta. La opción más segura para autenticarse en una máquina virtual Linux de Azure mediante SSH es con un par de claves pública y privada, también conocido como claves SSH. Más	AuditIfNotExists, Disabled	2.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	información: https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed.		
Los certificados deben tener el periodo de máximo de validez que se haya especificado	Administre los requisitos de cumplimiento de su organización. Para ello, especifique la cantidad máxima de tiempo que un certificado puede ser válido en el almacén de claves.	deshabilitado	2.1.0-preview
Implementar la extensión de configuración de invitado de Linux para permitir las asignaciones de configuración de invitado en máquinas virtuales Linux	Esta directiva implementa la extensión de configuración de invitado de Linux en las máquinas virtuales Linux hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Linux es un requisito previo para todas las asignaciones de configuración de invitado de Linux y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Linux. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Implementar la extensión de configuración de invitado de Windows para permitir las asignaciones de configuración de invitado en máquinas virtuales Windows	Esta directiva implementa la extensión de configuración de invitado de Windows en las máquinas virtuales Windows hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Windows es un requisito previo para todas las asignaciones de configuración de invitado de Windows y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Windows. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Las claves de Key Vault deben tener una fecha de expiración	Las claves criptográficas deben tener una fecha de expiración definida y no ser permanentes. Las claves que no expiran proporcionan a los posibles atacantes más tiempo para hacerse con ellas. Por ello, se recomienda como práctica de seguridad establecer fechas de expiración en las claves criptográficas.	Audit, Deny, Disabled	1.0.2
Los secretos de Key Vault deben tener una fecha de expiración	Los secretos deben tener una fecha de expiración definida y no ser permanentes. Los secretos que no expiran proporcionan a un posible atacante más tiempo para	Audit, Deny, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	ponerlos en peligro. Por ello, se recomienda como práctica de seguridad establecer fechas de expiración en los secretos.		
Control administrado por Microsoft 1317: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1318: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1319: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1320: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1321: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1322: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1323:	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
administración de autenticadores			
Control administrado por Microsoft 1324: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1325: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1326: administración de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticación basada en contraseñas

Id. : NIST SP 800-53 Rev. 4 IA-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado pero no tienen identidades administradas. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las	modify	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
de invitado en máquinas virtuales sin identidades	definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.		
Agregar una identidad administrada asignada por el sistema para habilitar las asignaciones de configuración de invitado en máquinas virtuales con una identidad asignada por el usuario	Esta directiva agrega una identidad administrada asignada por el sistema a las máquinas virtuales hospedadas en Azure que son compatibles con la configuración de invitado y que tienen al menos una identidad asignada por el usuario, pero no tienen ninguna identidad administrada asignada por el sistema. Una identidad administrada asignada por el sistema es un requisito previo para todas las asignaciones de configuración de invitado y debe agregarse a los equipos antes de usar las definiciones de directiva de la configuración de invitado. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	modify	1.0.0
Auditar las máquinas Linux que no tengan los permisos del archivo de contraseñas establecidos en 0644	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Linux no tienen los permisos del archivo de contraseñas establecidos en 0644.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows que permitan volver a usar las 24 contraseñas anteriores	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows permiten volver a usar las 24 contraseñas anteriores.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows cuyas contraseñas no tengan una vigencia máxima de 70 días	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no tienen una contraseña cuya duración máxima sea 70 días.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows cuyas contraseñas no tengan una vigencia mínima de 1 día	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no tienen una contraseña cuya duración mínima sea 1 día.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Auditar las máquinas Windows que no tengan habilitada la configuración de complejidad de la contraseña	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no tienen habilitada la configuración de complejidad de la contraseña.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows que no restrinjan la longitud mínima de las contraseñas a 14 caracteres	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no restringen la longitud mínima de la contraseña a 14 caracteres.	AuditIfNotExists, Disabled	1.0.0
Auditar las máquinas Windows que no almacenen contraseñas mediante cifrado reversible	Requiere que los requisitos previos se implementen en el ámbito de asignación de directivas. Para más detalles, visite https://aka.ms/gcpol. Las máquinas no son compatibles si las máquinas Windows no almacenan las contraseñas con cifrado reversible.	AuditIfNotExists, Disabled	1.0.0
Implementar la extensión de configuración de invitado de Linux para permitir las asignaciones de configuración de invitado en máquinas virtuales Linux	Esta directiva implementa la extensión de configuración de invitado de Linux en las máquinas virtuales Linux hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Linux es un requisito previo para todas las asignaciones de configuración de invitado de Linux y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Linux. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1
Implementar la extensión de configuración de invitado de Windows para permitir las asignaciones de configuración de invitado en máquinas virtuales Windows	Esta directiva implementa la extensión de configuración de invitado de Windows en las máquinas virtuales Windows hospedadas en Azure que son compatibles con la configuración de invitado. La extensión de configuración de invitado de Windows es un requisito previo para todas las asignaciones de configuración de invitado de Windows y debe implementarse en las máquinas antes de usar cualquier definición de directiva de configuración de invitado de Windows. Para más información sobre la configuración de invitado, visite https://aka.ms/gcpol.	deployIfNotExists	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1327: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1328: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1329: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1330: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1331: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1332: administración de autenticadores | Autenticación basada en contraseñas	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticación basada en PKI

Id. : NIST SP 800-53 Rev. 4 IA-5 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1333: administración de autenticadores | Autenticación basada en PKI	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1334: administración de autenticadores | Autenticación basada en PKI	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1335: administración de autenticadores | Autenticación basada en PKI	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0
Control administrado por Microsoft 1336: administración de autenticadores | Autenticación basada en PKI	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Registro de terceros en persona o de confianza

Id. : NIST SP 800-53 Rev. 4 IA-5 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1337: administración de autenticadores | Registro de terceros en persona o de confianza	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Compatibilidad automatizada para la determinación de la seguridad de la contraseña

Id. : NIST SP 800-53 Rev. 4 IA-5 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1338: administración de autenticadores | Compatibilidad automatizada para la determinación de la seguridad de la contraseña	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Protección de autenticadores

Id. : NIST SP 800-53 Rev. 4 IA-5 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1339: administración de autenticadores | Protección de autenticadores	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticadores estáticos no integrados sin cifrar

Id. : NIST SP 800-53 Rev. 4 IA-5 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1340: administración de autenticadores | Autenticadores estáticos no integrados sin cifrar	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Varias cuentas del sistema de información

Id. : NIST SP 800-53 Rev. 4 IA-5 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1341: administración de autenticadores | Varias cuentas del sistema de información	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticación basada en el token de hardware

Id. : NIST SP 800-53 Rev. 4 IA-5 (11)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1342: administración de autenticadores | Autenticación basada en el token de hardware	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Expiración de los autenticadores en caché

Id. : NIST SP 800-53 Rev. 4 IA-5 (13)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1343: administración de autenticadores | Expiración de los autenticadores en caché	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Comentarios de autenticador

Id. : NIST SP 800-53 Rev. 4 IA-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1344: comentarios del autenticador	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Autenticación del módulo criptográfico

Id. : NIST SP 800-53 Rev. 4 IA-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1345: autenticación de módulos criptográficos	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Identificación y autenticación (usuarios que no pertenecen a la organización)

Id. : NIST SP 800-53 Rev. 4 IA-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1346: identificación y autenticación (usuarios que no pertenecen a la organización)	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Aceptación de credenciales de PIV de otras agencias

Id. : NIST SP 800-53 Rev. 4 IA-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1347: identificación y autenticación (usuarios que no pertenecen a la organización) | Aceptación de credenciales de PIV de otras agencias	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Aceptación de credenciales de terceros

Id. : NIST SP 800-53 Rev. 4 IA-8 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1348: identificación y autenticación (usuarios que no pertenecen a la organización) | Aceptación de credenciales de terceros	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Uso de productos aprobados por FICAM

Id. : NIST SP 800-53 Rev. 4 IA-8 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1349: identificación y autenticación (usuarios que no pertenecen a la organización) | Uso de productos aprobados por FICAM	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Uso de perfiles emitidos por FICAM

Id. : NIST SP 800-53 Rev. 4 IA-8 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1350: identificación y autenticación (usuarios que no pertenecen a la organización) | Uso de perfiles emitidos por FICAM	Microsoft implementa este control de identificación y autenticación	auditoría	1.0.0

Respuesta a los incidentes

Procedimientos y directiva de respuesta a los incidentes

Id. : NIST SP 800-53 Rev. 4 IR-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1351: procedimientos y directiva de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1352: procedimientos y directiva de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Aprendizaje sobre la respuesta a los incidentes

Id. : NIST SP 800-53 Rev. 4 IR-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1353: aprendizaje sobre la respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1354: aprendizaje sobre la respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1355: aprendizaje sobre la respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Eventos simulados

Id. : NIST SP 800-53 Rev. 4 IR-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1356: aprendizaje sobre la respuesta a los incidentes | Eventos simulados	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Entornos de entrenamiento automatizado

Id. : NIST SP 800-53 Rev. 4 IR-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1357: aprendizaje sobre la respuesta a los incidentes | Entornos de entrenamiento automatizado	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Pruebas de la respuesta a los incidentes

Id. : NIST SP 800-53 Rev. 4 IR-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1358: pruebas de la respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Coordinación con planes relacionados

Id. : NIST SP 800-53 Rev. 4 IR-3 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1359: pruebas de la respuesta a los incidentes | Coordinación con planes relacionados	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Tratamiento de incidentes

Id. : NIST SP 800-53 Rev. 4 IR-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La opción para enviar notificaciones por correo electrónico para alertas de gravedad alta debe estar habilitada.	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, habilite las notificaciones por correo electrónico de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	1.0.1
La opción para enviar notificaciones por correo electrónico al propietario de la suscripción en relación a alertas de gravedad alta debe estar habilitada.	Para asegurarse de que los propietarios de suscripciones reciban una notificación cuando se produzca una vulneración de seguridad potencial en sus suscripciones, establezca notificaciones por correo electrónico a los propietarios de las suscripciones de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	2.0.0
Control administrado por Microsoft 1360: control de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1361: control de	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
incidentes			
Control administrado por Microsoft 1362: control de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Las suscripciones deben tener una dirección de correo electrónico de contacto para los problemas de seguridad	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, establezca un contacto de seguridad para la recepción de notificaciones por correo electrónico de Security Center.	AuditIfNotExists, Disabled	1.0.1

Procesos automatizados de control de incidentes

Id. : NIST SP 800-53 Rev. 4 IR-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1363: control de incidentes | Procesos automatizados de control de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Reconfiguración dinámica

Id. : NIST SP 800-53 Rev. 4 IR-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1364: control de incidentes | Reconfiguración dinámica	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Continuidad de las operaciones

Id. : NIST SP 800-53 Rev. 4 IR-4 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1365: control de incidentes | Continuidad de las operaciones	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Correlación de la información

Id. : NIST SP 800-53 Rev. 4 IR-4 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1366: control de incidentes | Correlación de la información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Amenazas internas: funcionalidades específicas

Id. : NIST SP 800-53 Rev. 4 IR-4 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1367: control de incidentes | Amenazas internas: funcionalidades específicas	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Correlación con organizaciones externas

Id. : NIST SP 800-53 Rev. 4 IR-4 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1368: control de incidentes | Correlación con organizaciones externas	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Supervisión de incidentes

Id. : NIST SP 800-53 Rev. 4 IR-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La opción para enviar notificaciones por correo electrónico para alertas de gravedad alta debe estar habilitada.	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, habilite las notificaciones por correo electrónico de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La opción para enviar notificaciones por correo electrónico al propietario de la suscripción en relación a alertas de gravedad alta debe estar habilitada.	Para asegurarse de que los propietarios de suscripciones reciban una notificación cuando se produzca una vulneración de seguridad potencial en sus suscripciones, establezca notificaciones por correo electrónico a los propietarios de las suscripciones de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	2.0.0
Control administrado por Microsoft 1369: supervisión de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Las suscripciones deben tener una dirección de correo electrónico de contacto para los problemas de seguridad	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, establezca un contacto de seguridad para la recepción de notificaciones por correo electrónico de Security Center.	AuditIfNotExists, Disabled	1.0.1

Seguimiento automatizado, recopilación de datos o análisis

Id. : NIST SP 800-53 Rev. 4 IR-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1370: supervisión de incidentes | Seguimiento automatizado, recopilación de datos o análisis	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Informes de incidentes

Id. : NIST SP 800-53 Rev. 4 IR-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1371: informes de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1372: informes de incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Informes automatizados

Id. : NIST SP 800-53 Rev. 4 IR-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1373: informes de incidentes | Informes automatizados	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Vulnerabilidades relacionadas con incidentes

Id. : NIST SP 800-53 Rev. 4 IR-6 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La opción para enviar notificaciones por correo electrónico para alertas de	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de	AuditIfNotExists, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
gravedad alta debe estar habilitada.	seguridad potencial en una de las suscripciones, habilite las notificaciones por correo electrónico de alertas de gravedad alta en Security Center.		
La opción para enviar notificaciones por correo electrónico al propietario de la suscripción en relación a alertas de gravedad alta debe estar habilitada.	Para asegurarse de que los propietarios de suscripciones reciban una notificación cuando se produzca una vulneración de seguridad potencial en sus suscripciones, establezca notificaciones por correo electrónico a los propietarios de las suscripciones de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	2.0.0
Las suscripciones deben tener una dirección de correo electrónico de contacto para los problemas de seguridad	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, establezca un contacto de seguridad para la recepción de notificaciones por correo electrónico de Security Center.	AuditIfNotExists, Disabled	1.0.1

Ayuda para la respuesta a los incidentes

Id. : NIST SP 800-53 Rev. 4 IR-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1374: ayuda para la respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Compatibilidad automatizada para la disponibilidad de la información o soporte técnico

Id. : NIST SP 800-53 Rev. 4 IR-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1375: ayuda para la respuesta a los incidentes | Compatibilidad automatizada para la disponibilidad de la información o soporte técnico	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Coordinación con proveedores externos

Id. : NIST SP 800-53 Rev. 4 IR-7 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1376: ayuda para la respuesta a los incidentes | Coordinación con proveedores externos	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1377: ayuda para la respuesta a los incidentes | Coordinación con proveedores externos	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Plan de respuesta a los incidentes

Id. : NIST SP 800-53 Rev. 4 IR-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1378: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1379: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1380: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1381: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1382: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1383: plan de respuesta a los incidentes	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Respuesta a derrames de información

Id. : NIST SP 800-53 Rev. 4 IR-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1384: respuesta a filtraciones de información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1385: respuesta a filtraciones de información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1386: respuesta a filtraciones de	Microsoft implementa este control de respuesta a los	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
información	incidentes		
Control administrado por Microsoft 1387: respuesta a filtraciones de información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1388: respuesta a filtraciones de información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0
Control administrado por Microsoft 1389: respuesta a filtraciones de información	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Personal responsable

Id. : NIST SP 800-53 Rev. 4 IR-9 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1390: respuesta a filtraciones de información | Personal responsable	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Cursos

Id. : NIST SP 800-53 Rev. 4 IR-9 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1391: respuesta a filtraciones de información | Cursos	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Operaciones posteriores al volcado

Id. : NIST SP 800-53 Rev. 4 IR-9 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1392: respuesta a filtraciones de información | Operaciones posteriores al volcado	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Exposición a personal no autorizado

Id. : NIST SP 800-53 Rev. 4 IR-9 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1393: respuesta a filtraciones de información | Exposición a personal no autorizado	Microsoft implementa este control de respuesta a los incidentes	auditoría	1.0.0

Mantenimiento

Procedimientos y directiva de mantenimiento del sistema

Id. : NIST SP 800-53 Rev. 4 MA-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1394: procedimientos y directiva de mantenimiento del sistema	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1395: procedimientos y directiva de mantenimiento del sistema	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Mantenimiento controlado

Id. : NIST SP 800-53 Rev. 4 MA-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1396: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1397: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1398: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1399: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1400: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1401: mantenimiento controlado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Actividades de mantenimiento automatizado

Id. : NIST SP 800-53 Rev. 4 MA-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1402: mantenimiento controlado | Actividades de mantenimiento automatizado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1403: mantenimiento controlado | Actividades de mantenimiento automatizado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Herramientas de mantenimiento

Id. : NIST SP 800-53 Rev. 4 MA-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1404: herramientas de mantenimiento	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Inspección de herramientas

Id. : NIST SP 800-53 Rev. 4 MA-3 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1405: herramientas de mantenimiento | Inspección de herramientas	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Inspección del soporte físico

Id. : NIST SP 800-53 Rev. 4 MA-3 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1406: herramientas de mantenimiento | Inspección del soporte físico	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Impedir la eliminación no autorizada

Id. : NIST SP 800-53 Rev. 4 MA-3 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1407: herramientas de mantenimiento | Impedir la eliminación no autorizada	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1408: herramientas de mantenimiento | Impedir la eliminación no autorizada	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1409: herramientas de mantenimiento | Impedir la eliminación no autorizada	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1410: herramientas de mantenimiento | Impedir la eliminación no autorizada	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Mantenimiento no local

Id. : NIST SP 800-53 Rev. 4 MA-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1411: mantenimiento no local	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1412: mantenimiento no local	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1413: mantenimiento no local	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1414: mantenimiento no local	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1415: mantenimiento no local	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Mantenimiento no local de documentos

Id. : NIST SP 800-53 Rev. 4 MA-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1416: mantenimiento no local | Mantenimiento no local de documentos	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Seguridad o saneamiento comparable

Id. : NIST SP 800-53 Rev. 4 MA-4 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1417: mantenimiento no local | Seguridad o saneamiento comparable	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1418: mantenimiento no local | Seguridad o saneamiento comparable	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Protección criptográfica

Id. : NIST SP 800-53 Rev. 4 MA-4 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1419: mantenimiento no local | Protección criptográfica	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Personal de mantenimiento

Id. : NIST SP 800-53 Rev. 4 MA-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1420: personal de mantenimiento	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1421: personal de mantenimiento	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1422: personal de mantenimiento	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Personas sin acceso adecuado

Id. : NIST SP 800-53 Rev. 4 MA-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1423: personal de mantenimiento | Personas sin acceso adecuado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0
Control administrado por Microsoft 1424: personal de mantenimiento | Personas sin acceso adecuado	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Mantenimiento temporal

Id. : NIST SP 800-53 Rev. 4 MA-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1425: mantenimiento puntual	Microsoft implementa este control de mantenimiento	auditoría	1.0.0

Protección de elementos multimedia

Procedimientos y directivas de protección de medios

Id. : NIST SP 800-53 Rev. 4 MP-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1426: procedimientos y directiva de protección de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1427: procedimientos y directiva de protección de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Acceso a medios

Id. : NIST SP 800-53 Rev. 4 MP-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1428: acceso a elementos	Microsoft implementa este control de protección de	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
multimedia	elementos multimedia		

Marcado de medios

Id. : NIST SP 800-53 Rev. 4 MP-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1429: marcado de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1430: marcado de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Almacenamiento de medios

Id. : NIST SP 800-53 Rev. 4 MP-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1431: almacenamiento de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1432: almacenamiento de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Transporte de medios

Id. : NIST SP 800-53 Rev. 4 MP-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1433: transporte de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1434: transporte de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1435: transporte de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1436: transporte de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Protección criptográfica

Id. : NIST SP 800-53 Rev. 4 MP-5 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1437: transporte de elementos multimedia | Protección criptográfica	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Saneamiento de medios

Id. : NIST SP 800-53 Rev. 4 MP-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1438: saneamiento de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0
Control administrado por Microsoft 1439: saneamiento de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Revisión, aprobación, seguimiento, documentación y comprobación

Id. : NIST SP 800-53 Rev. 4 MP-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1440: saneamiento de elementos multimedia | Revisión, aprobación, seguimiento, documentación y comprobación	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Pruebas de equipos

Id. : NIST SP 800-53 Rev. 4 MP-6 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1441: saneamiento de elementos multimedia | Pruebas de equipos	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Técnicas no destructivas

Id. : NIST SP 800-53 Rev. 4 MP-6 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1442: saneamiento de elementos multimedia | Técnicas no destructivas	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Uso de los medios

Id. : NIST SP 800-53 Rev. 4 MP-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1443: uso de elementos multimedia	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Prohibir el uso sin propietario

Id. : NIST SP 800-53 Rev. 4 MP-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1444: uso de medios | Prohibir el uso sin propietario	Microsoft implementa este control de protección de elementos multimedia	auditoría	1.0.0

Protección física y del entorno

Procedimientos y directivas de protección física y del entorno

Id. : NIST SP 800-53 Rev. 4 PE-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1445: procedimientos y directivas de protección física y del entorno	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1446: procedimientos y directivas de protección física y del entorno	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Autorizaciones de acceso físico

Id. : NIST SP 800-53 Rev. 4 PE-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1447: autorizaciones de acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1448: autorizaciones de acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1449: autorizaciones de acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1450: autorizaciones de acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Control de acceso físico

Id. : NIST SP 800-53 Rev. 4 PE-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1451: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1452: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1453: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1454: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1455: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1456: control del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1457: control del acceso	Microsoft implementa este control de protección física y del	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
físico	entorno		

Acceso al sistema de información

Id. : NIST SP 800-53 Rev. 4 PE-3 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1458: control del acceso físico | Acceso al sistema de información	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Control de acceso para medios de transmisión

Id. : NIST SP 800-53 Rev. 4 PE-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1459: control de acceso para medios de transmisión	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Control de acceso para los dispositivos de salida

Id. : NIST SP 800-53 Rev. 4 PE-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1460: control de acceso para dispositivos de salida	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Supervisión del acceso físico

Id. : NIST SP 800-53 Rev. 4 PE-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1461: supervisión del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1462: supervisión del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1463: supervisión del acceso físico	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Dispositivos de vigilancia o alarmas de intrusión

Id. : NIST SP 800-53 Rev. 4 PE-6 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1464: supervisión del acceso físico | Dispositivos de vigilancia o alarmas de intrusión	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Supervisión del acceso físico a los sistemas de información

Id. : NIST SP 800-53 Rev. 4 PE-6 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1465: supervisión del acceso físico | Supervisión del acceso físico a los sistemas de información	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Registros de acceso de los visitantes

Id. : NIST SP 800-53 Rev. 4 PE-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1466: registros de acceso de los visitantes	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1467: registros de acceso de los visitantes	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Mantenimiento o revisión de registros automatizados

Id. : NIST SP 800-53 Rev. 4 PE-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1468: registros de acceso de los visitantes | Mantenimiento o revisión de registros automatizados	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Equipamiento electrónico y cableado de alimentación

Id. : NIST SP 800-53 Rev. 4 PE-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1469: equipamiento y cableado de alimentación	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Interrupción de emergencia

Id. : NIST SP 800-53 Rev. 4 PE-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1470: interrupción de emergencia	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1471: interrupción de emergencia	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1472: interrupción de emergencia	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Alimentación de emergencia

Id. : NIST SP 800-53 Rev. 4 PE-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1473: alimentación de emergencia	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Suministro eléctrico alternativo a largo plazo: capacidad operativa mínima

Id. : NIST SP 800-53 Rev. 4 PE-11 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1474: alimentación de emergencia | Suministro eléctrico alternativo a largo plazo: capacidad operativa mínima	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Iluminación de emergencia

Id. : NIST SP 800-53 Rev. 4 PE-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1475: iluminación de emergencia	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Protección contra incendios

Id. : NIST SP 800-53 Rev. 4 PE-13

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1476: protección contra incendios	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Dispositivos o sistemas de detección

Id. : NIST SP 800-53 Rev. 4 PE-13 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1477: protección contra incendios | Dispositivos o sistemas de detección	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Dispositivos o sistemas de eliminación

Id. : NIST SP 800-53 Rev. 4 PE-13 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1478: protección contra incendios | Dispositivos o sistemas de eliminación	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Extinción automática de incendios

Id. : NIST SP 800-53 Rev. 4 PE-13 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1479: protección contra incendios | Extinción automática de incendios	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Controles de temperatura y humedad

Id. : NIST SP 800-53 Rev. 4 PE-14

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1480: controles de temperatura y humedad	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1481: controles de temperatura y humedad	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Supervisión con alarmas o notificaciones

Id. : NIST SP 800-53 Rev. 4 PE-14 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1482: controles de temperatura y humedad | Supervisión con alarmas o notificaciones	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Protección contra daños por el agua

Id. : NIST SP 800-53 Rev. 4 PE-15

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1483: protección contra daños por el agua	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

compatibilidad con automatización

Id. : NIST SP 800-53 Rev. 4 PE-15 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1484: protección contra daños por el agua | Compatibilidad con la automatización	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Entrega y eliminación

Id. : NIST SP 800-53 Rev. 4 PE-16

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1485: entrega y eliminación	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Lugar de trabajo alternativo

Id. : NIST SP 800-53 Rev. 4 PE-17

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1486: sitio de trabajo alternativo	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0
Control administrado por Microsoft 1487: sitio de trabajo alternativo	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1488: sitio de trabajo alternativo	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Ubicación de los componentes del sistema de información

Id. : NIST SP 800-53 Rev. 4 PE-18

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1489: ubicación de los componentes del sistema de información	Microsoft implementa este control de protección física y del entorno	auditoría	1.0.0

Planificación

Procedimientos y directiva del planeamiento de la seguridad

Id. : NIST SP 800-53 Rev. 4 PL-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1490: procedimientos y directiva del planeamiento de la seguridad	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1491: procedimientos y directiva del planeamiento de la seguridad	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Plan de seguridad del sistema

Id. : NIST SP 800-53 Rev. 4 PL-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1492: plan de seguridad del sistema	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1493: plan de seguridad del sistema	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1494: plan de seguridad del sistema	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1495: plan de seguridad del sistema	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1496: plan de seguridad del sistema	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Planificación o coordinación con otras entidades organizativas

Id. : NIST SP 800-53 Rev. 4 PL-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1497: plan de seguridad del sistema | Plan o coordinación con otras entidades organizativas	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Reglas de comportamiento

Id. : NIST SP 800-53 Rev. 4 PL-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1498: reglas de comportamiento	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1499: reglas de comportamiento	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1500: reglas de comportamiento	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1501: reglas de comportamiento	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Restricciones de medios y redes sociales

Id. : NIST SP 800-53 Rev. 4 PL-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1502: reglas de comportamiento | Restricciones de medios y redes sociales	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Arquitectura de seguridad de la información

Id. : NIST SP 800-53 Rev. 4 PL-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1503: arquitectura de seguridad de la información	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1504: arquitectura de seguridad de la información	Microsoft implementa este control de planeamiento	auditoría	1.0.0
Control administrado por Microsoft 1505: arquitectura de seguridad de la información	Microsoft implementa este control de planeamiento	auditoría	1.0.0

Seguridad del personal

Procedimientos y directiva de seguridad del personal

Id. : NIST SP 800-53 Rev. 4 PS-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1506: procedimientos y directiva de seguridad del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1507: procedimientos y directiva de seguridad del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Designación de riesgos de puestos

Id. : NIST SP 800-53 Rev. 4 PS-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1508: designación de riesgos de puestos	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1509: designación de riesgos de puestos	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1510: designación de riesgos de puestos	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Filtrado del personal

Id. : NIST SP 800-53 Rev. 4 PS-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1511: filtrado del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1512: filtrado del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Información con medidas de protección especiales

Id. : NIST SP 800-53 Rev. 4 PS-3 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1513: filtrado del personal | Información con medidas de protección especiales	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1514: filtrado del personal | Información con medidas de protección especiales	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Finalización del contrato del personal

Id. : NIST SP 800-53 Rev. 4 PS-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1515: finalización del contrato del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1516: finalización del contrato del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1517: finalización del contrato del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1518: finalización del contrato del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1519: finalización del contrato del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1520: finalización del contrato del	Microsoft implementa este control de seguridad del	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
personal	personal		

Notificación automatizada

Id. : NIST SP 800-53 Rev. 4 PS-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1521: finalización del contrato del personal | Notificación automatizada	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Transferencia de personal

Id. : NIST SP 800-53 Rev. 4 PS-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1522: transferencia de personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1523: transferencia de personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1524: transferencia de personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1525: transferencia de personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Contratos de acceso

Id. : NIST SP 800-53 Rev. 4 PS-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1526: contratos de acceso	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1527: contratos de acceso	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1528: contratos de acceso	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Seguridad del personal de terceros

Id. : NIST SP 800-53 Rev. 4 PS-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1529: seguridad del personal de terceros	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1530: seguridad del personal de	Microsoft implementa este control de seguridad del	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
terceros	personal		
Control administrado por Microsoft 1531: seguridad del personal de terceros	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1532: seguridad del personal de terceros	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1533: seguridad del personal de terceros	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Sanciones del personal

Id. : NIST SP 800-53 Rev. 4 PS-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1534: sanciones del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0
Control administrado por Microsoft 1535: sanciones del personal	Microsoft implementa este control de seguridad del personal	auditoría	1.0.0

Evaluación de riesgos

Directiva de evaluación de riesgos y procedimientos

Id. : NIST SP 800-53 Rev. 4 RA-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1536: directiva y procedimientos de evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1537: directiva y procedimientos de evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Categorización de seguridad

Id. : NIST SP 800-53 Rev. 4 RA-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1538: categorización de la seguridad	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1539: categorización de la seguridad	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1540: categorización de la seguridad	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Evaluación de riesgos

Id. : NIST SP 800-53 Rev. 4 RA-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1541: evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1542: evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1543: evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1544: evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1545: evaluación de riesgos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Examen de vulnerabilidades

Id. : NIST SP 800-53 Rev. 4 RA-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe habilitarse una solución de evaluación de vulnerabilidades en sus máquinas virtuales	Audita las máquinas virtuales para detectar si ejecutan una solución de evaluación de vulnerabilidades admitida. Un componente fundamental de cada programa de seguridad y riesgo cibernético es la identificación y el análisis de las vulnerabilidades. El plan de tarifa estándar de Azure Security Center incluye el análisis de vulnerabilidades de las máquinas virtuales sin costo adicional. Además, Security Center puede implementar automáticamente esta herramienta.	AuditIfNotExists, Disabled	3.0.0
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure SQL Database	indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.		
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
Control administrado por Microsoft 1546: examen de vulnerabilidades	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1547: examen de vulnerabilidades	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1548: examen de	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
vulnerabilidades			
Control administrado por Microsoft 1549: examen de vulnerabilidades	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Control administrado por Microsoft 1550: examen de vulnerabilidades	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0
Las bases de datos SQL deben tener resueltos los hallazgos de vulnerabilidades.	Permite supervisar los resultados del examen de evaluación de puntos vulnerables y las recomendaciones para solucionar los de las bases de datos.	AuditIfNotExists, Disabled	4.0.0
Los servidores SQL de las máquinas deben tener resueltos los hallazgos de vulnerabilidades.	La evaluación de vulnerabilidades de SQL examina la base de datos en busca de vulnerabilidades de seguridad y expone las posibles desviaciones de los procedimientos recomendados, como errores de configuración, permisos excesivos y datos confidenciales sin protección. La corrección de las vulnerabilidades detectadas puede mejorar considerablemente la posición de seguridad de la base de datos.	AuditIfNotExists, Disabled	1.0.0
Se deben corregir las vulnerabilidades de las imágenes de Azure Container Registry	La evaluación de vulnerabilidades de la imagen de contenedor examina el registro en busca de vulnerabilidades de seguridad en cada imagen de contenedor insertada y expone resultados detallados de cada imagen (con la tecnología de Qualys). La resolución de las vulnerabilidades puede mejorar considerablemente la posición de seguridad de los contenedores y protegerlos frente a ataques.	AuditIfNotExists, Disabled	2.0.0
Las vulnerabilidades en las configuraciones de seguridad de contenedor deben corregirse	Audite las vulnerabilidades en la configuración de seguridad de las máquinas con Docker instalado y muéstrelas como recomendaciones en Azure Security Center.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se deben corregir las vulnerabilidades en la configuración de seguridad en las máquinas	Azure Security Center supervisará los servidores que no cumplan la línea de base configurada como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
Se deben corregir las vulnerabilidades en la configuración de seguridad de los conjuntos de escalado de máquinas virtuales	Audite las vulnerabilidades del sistema operativo en los conjuntos de escalado de máquinas virtuales para protegerlos frente a ataques.	AuditIfNotExists, Disabled	3.0.0
La evaluación de vulnerabilidades debe estar habilitada en Instancia administrada de SQL	Audita cada servicio SQL Managed Instance que no tiene habilitado los exámenes de evaluación de vulnerabilidades periódicos. La evaluación de vulnerabilidades permite detectar las vulnerabilidades potenciales de la base de datos, así como hacer un seguimiento y ayudar a corregirlas.	AuditIfNotExists, Disabled	1.0.1
La evaluación de vulnerabilidades debe estar activada en sus servidores de SQL Server	Audita los servidores Azure SQL Server que no tienen habilitados los exámenes de evaluación de vulnerabilidades periódicos. La evaluación de vulnerabilidades permite detectar las vulnerabilidades potenciales de la base de datos, así como hacer un seguimiento y ayudar a corregirlas.	AuditIfNotExists, Disabled	2.0.0
La evaluación de vulnerabilidades debe estar habilitada en las áreas de trabajo de Synapse	Para detectar, seguir y corregir posibles vulnerabilidades, configure exámenes periódicos de evaluación de las vulnerabilidades de SQL en las áreas de trabajo de Synapse.	AuditIfNotExists, Disabled	1.0.0

Funcionalidad de la herramienta de actualización

Id. : NIST SP 800-53 Rev. 4 RA-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1551: examen de vulnerabilidades | Funcionalidad de la herramienta de actualización	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Actualización por frecuencia o antes de nuevo análisis, o cuando se identifique

Id. : NIST SP 800-53 Rev. 4 RA-5 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1552: examen de vulnerabilidades | Actualización por frecuencia o antes de nuevo análisis, o cuando se identifique	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Amplitud o profundidad de cobertura

Id. : NIST SP 800-53 Rev. 4 RA-5 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1553: examen de vulnerabilidades | Amplitud o profundidad de cobertura	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Información detectable

Id. : NIST SP 800-53 Rev. 4 RA-5 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1554: examen de vulnerabilidades | Información detectable	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Acceso con privilegios

Id. : NIST SP 800-53 Rev. 4 RA-5 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1555: examen de vulnerabilidades | Acceso con privilegios	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Análisis de tendencias automatizados

Id. : NIST SP 800-53 Rev. 4 RA-5 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1556: examen de vulnerabilidades | Análisis de tendencias automatizados	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Revisión de registros de auditoría históricos

Id. : NIST SP 800-53 Rev. 4 RA-5 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1557: examen de vulnerabilidades | Revisión de registros de auditoría históricos	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Correlación de información de examen

Id. : NIST SP 800-53 Rev. 4 RA-5 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1558: examen de vulnerabilidades | Correlación de información de examen	Microsoft implementa este control de evaluación de riesgos	auditoría	1.0.0

Adquisición del sistema y los servicios

Procedimientos y directiva de adquisición del sistema y los servicios

Id. : NIST SP 800-53 Rev. 4 SA-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1559: procedimientos y directiva de	Microsoft implementa este control de adquisición	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
adquisición del sistema y los servicios	del sistema y los servicios		
Control administrado por Microsoft 1560: procedimientos y directiva de adquisición del sistema y los servicios	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Asignación de recursos

Id. : NIST SP 800-53 Rev. 4 SA-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1561: asignación de recursos	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1562: asignación de recursos	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1563: asignación de recursos	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Ciclo de vida del desarrollo del sistema

Id. : NIST SP 800-53 Rev. 4 SA-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1564: ciclo de vida del desarrollo del sistema	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1565: ciclo de vida del desarrollo del sistema	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1566: ciclo de vida del desarrollo del sistema	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1567: ciclo de vida del desarrollo del sistema	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Proceso de adquisición

Id. : NIST SP 800-53 Rev. 4 SA-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1568: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1569: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1570: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1571: proceso de	Microsoft implementa este control de adquisición del sistema y	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
adquisición	los servicios		
Control administrado por Microsoft 1572: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1573: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1574: proceso de adquisición	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Propiedades funcionales de controles de seguridad

Id. : NIST SP 800-53 Rev. 4 SA-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1575: proceso de adquisición | Propiedades funcionales de controles de seguridad	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Información de diseño e implementación para controles de seguridad

Id. : NIST SP 800-53 Rev. 4 SA-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1576: proceso de adquisición | Información de diseño e implementación para controles de seguridad	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Plan de supervisión continua

Id. : NIST SP 800-53 Rev. 4 SA-4 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1577: proceso de adquisición | Plan de supervisión continua	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Funciones, puertos, protocolos, servicios en uso

Id. : NIST SP 800-53 Rev. 4 SA-4 (9)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1578: proceso de adquisición | Funciones, puertos, protocolos, servicios en uso	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Uso de productos PIV aprobados

Id. : NIST SP 800-53 Rev. 4 SA-4 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1579: proceso de adquisición | Uso de productos PIV aprobados	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Documentación del sistema de información

Id. : NIST SP 800-53 Rev. 4 SA-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1580: documentación del sistema de información	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1581: documentación del sistema de información	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1582: documentación del sistema de información	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1583: documentación del sistema de información	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1584: documentación del sistema de información	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Principios de ingeniería de seguridad

Id. : NIST SP 800-53 Rev. 4 SA-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1585: principios de ingeniería de seguridad	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Servicios del sistema de información externo

Id. : NIST SP 800-53 Rev. 4 SA-9

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1586: servicios del sistema de información externo	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1587: servicios del sistema de información externo	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1588: servicios del sistema de información externo	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Evaluaciones de riesgos o aprobaciones de la organización

Id. : NIST SP 800-53 Rev. 4 SA-9 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1589: servicios del sistema de información externo | Evaluaciones de riesgos o aprobaciones de la organización	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1590: servicios del sistema de información externo | Evaluaciones de riesgos o aprobaciones de la organización	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Identificación de funciones, puertos, protocolos o servicios

Id. : NIST SP 800-53 Rev. 4 SA-9 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1591: servicios del sistema de información externo | Identificación de funciones, puertos, protocolos o servicios	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Intereses coherentes de consumidores y proveedores

Id. : NIST SP 800-53 Rev. 4 SA-9 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1592: servicios del sistema de información externo | Intereses coherentes de consumidores y proveedores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Procesamiento, almacenamiento y ubicación del servicio

Id. : NIST SP 800-53 Rev. 4 SA-9 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1593: servicios del sistema de información externo | Procesamiento, almacenamiento y ubicación del servicio	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Administración de configuración para desarrolladores

Id. : NIST SP 800-53 Rev. 4 SA-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1594: administración de configuración para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1595: administración de configuración para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1596: administración de configuración para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1597: administración de configuración para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1598: administración de configuración para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Comprobación de integridad de software o firmware

Id. : NIST SP 800-53 Rev. 4 SA-10 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1599: administración de configuración para desarrolladores | Comprobación de integridad de software o firmware	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Pruebas y evaluación de la seguridad para desarrolladores

Id. : NIST SP 800-53 Rev. 4 SA-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1600: pruebas y evaluación de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1601: pruebas y evaluación de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1602: pruebas y evaluación de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1603: pruebas y evaluación de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1604: pruebas y evaluación de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Análisis de código estático

Id. : NIST SP 800-53 Rev. 4 SA-11 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1605: pruebas y evaluación de la seguridad para desarrolladores | Análisis de código estático	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Análisis de amenazas y vulnerabilidades

Id. : NIST SP 800-53 Rev. 4 SA-11 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1606: pruebas y evaluación de la seguridad para desarrolladores | Análisis de amenazas y vulnerabilidades	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Análisis de código dinámico

Id. : NIST SP 800-53 Rev. 4 SA-11 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1607: pruebas y evaluación de la seguridad para desarrolladores | Análisis de código dinámico	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Protección de la cadena de suministro

Id. : NIST SP 800-53 Rev. 4 SA-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1608: protección de la cadena de suministro	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Proceso de desarrollo, estándares y herramientas

Id. : NIST SP 800-53 Rev. 4 SA-15

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1609: proceso de desarrollo, estándares y herramientas	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1610: proceso de desarrollo, estándares y herramientas	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Entrenamiento proporcionado por desarrolladores

Id. : NIST SP 800-53 Rev. 4 SA-16

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1611: aprendizaje proporcionado por el desarrollador	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Diseño y arquitectura de la seguridad para desarrolladores

Id. : NIST SP 800-53 Rev. 4 SA-17

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1612: diseño y arquitectura de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1613: diseño y arquitectura de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0
Control administrado por Microsoft 1614: diseño y arquitectura de la seguridad para desarrolladores	Microsoft implementa este control de adquisición del sistema y los servicios	auditoría	1.0.0

Protección del sistema y de las comunicaciones

Directiva y procedimientos para la protección del sistema y de las comunicaciones

Id. : NIST SP 800-53 Rev. 4 SC-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1615: directiva y procedimientos para la protección del sistema y de las comunicaciones	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1616: directiva y procedimientos para la protección del sistema y de las comunicaciones	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Creación de particiones en la aplicación

Id. : NIST SP 800-53 Rev. 4 SC-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1617: creación de particiones en la aplicación	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Aislamiento de la función de seguridad

Id. : NIST SP 800-53 Rev. 4 SC-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La solución de protección del punto de conexión debe instalarse en las máquinas virtuales	Audite la existencia y el estado de una solución de protección de puntos de conexión en los conjuntos de escalado de máquinas virtuales para protegerlos frente a amenazas y vulnerabilidades.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1618: aislamiento de la función de seguridad	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Supervisar la falta de Endpoint Protection en Azure Security Center	Azure Security Center supervisará los servidores sin un agente de Endpoint Protection instalado como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
La Protección contra vulnerabilidades de seguridad de Windows Defender debe estar habilitada en las máquinas .	La protección contra vulnerabilidades de seguridad de Windows Defender utiliza el agente de configuración de invitado de Azure Policy. La protección contra vulnerabilidades de seguridad tiene cuatro componentes diseñados para bloquear dispositivos en una amplia variedad de vectores de ataque y comportamientos de bloque utilizados habitualmente en ataques de malware, al tiempo que permiten a las empresas equilibrar los requisitos de productividad y riesgo de seguridad (solo Windows).	AuditIfNotExists, Disabled	1.1.1

Información en recursos compartidos

Id. : NIST SP 800-53 Rev. 4 SC-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1619: información en recursos compartidos	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Protección ante la denegación de servicio

Id. : NIST SP 800-53 Rev. 4 SC-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure DDoS Protection debe estar habilitado	DDoS Protection debe estar habilitado en todas las redes virtuales que tengan una subred que forme parte de una puerta de enlace de aplicación con una IP pública.	AuditIfNotExists, Disabled	3.0.0
El reenvío de IP en la máquina virtual debe estar deshabilitado	Habilitar el reenvío de IP en la NIC de la máquina virtual permite que la máquina reciba tráfico dirigido a otros destinos. El reenvío de IP rara vez es necesario (por ejemplo, cuando se usa la máquina virtual como una aplicación virtual de red) y, por lo tanto, el equipo de seguridad de red debe revisarlo.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1620: protección contra la denegación de servicio	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
El firewall de aplicaciones web (WAF) debe estar habilitado para Application Gateway	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.		
Web Application Firewall (WAF) debe estar habilitado en el servicio Azure Front Door Service	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.	Audit, Deny, Disabled	1.0.1

Disponibilidad de recursos

Id. : NIST SP 800-53 Rev. 4 SC-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1621: disponibilidad de recursos	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Protección de límites

Id. : NIST SP 800-53 Rev. 4 SC-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las recomendaciones de protección de red adaptable se deben aplicar en las máquinas virtuales accesibles desde Internet	Azure Security Center analiza los patrones de tráfico de máquinas virtuales orientadas a Internet y proporciona recomendaciones de reglas de grupo de seguridad de red que reducen la superficie de ataque potencial.	AuditIfNotExists, Disabled	3.0.0
Todo el tráfico de Internet debe enrutarse mediante la instancia de Azure Firewall implementada	Azure Security Center ha identificado que algunas de las subredes no están protegidas con un firewall de próxima generación. Proteja las subredes frente a posibles amenazas mediante la restricción del acceso a ellas con Azure Firewall o un firewall de próxima generación compatible.	AuditIfNotExists, Disabled	3.0.0-preview
Todos los puertos de red deben estar restringidos en los grupos de seguridad de red asociados a la máquina virtual	Azure Security Center identificó que algunas de las reglas de entrada de sus grupos de seguridad de red son demasiado permisivas. Las reglas de entrada no deben permitir el acceso desde los intervalos "Cualquiera" o "Internet". Esto podría permitir que los atacantes pudieran acceder a sus recursos.	AuditIfNotExists, Disabled	3.0.0
Los servicios de API Management deben usar una red virtual	La implementación de Azure Virtual Network ofrece una seguridad y aislamiento mejorados, y permite colocar el servicio de API Management en una red enrutable sin conexión a Internet cuyo acceso puede controlar. Estas redes se pueden conectar a las redes locales mediante diversas tecnologías de VPN, lo que permite el acceso a los servicios de back-end dentro de la red o de forma local. El portal para desarrolladores y la puerta de enlace de API pueden configurarse para que sea accesible desde Internet o solo dentro de la red virtual.	Audit, Disabled	1.0.1
App Configuration debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a las instancias de App Configuration en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/appconfig/private-endpoint.	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los intervalos IP autorizados deben definirse en los servicios de Kubernetes	Restrinja el acceso a la API de administración de servicios de Kubernetes mediante la concesión de acceso de API solo a direcciones IP en intervalos específicos. Se recomienda limitar el acceso a los intervalos IP autorizados para garantizar que solo las aplicaciones de las redes permitidas puedan acceder al clúster.	Audit, Disabled	2.0.1
Azure API for FHIR debe usar un vínculo privado.	Azure API for FHIR debe tener al menos una conexión de punto de conexión privado aprobada. Los clientes de una red virtual pueden acceder de forma segura a los recursos que tengan conexiones de punto de conexión privadas mediante vínculos privados. Para más información, visite https://aka.ms/fhir-privatelink.	Audit, Disabled	1.0.0
Azure Cache for Redis debe usar Private Link	Los puntos de conexión privados le permiten conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. Al asignar puntos de conexión privados a las instancias de Azure Cache for Redis, se reduce el riesgo de pérdida de datos. Más información en: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link.	AuditIfNotExists, Disabled	1.0.0
El servicio Azure Cognitive Search debe usar una SKU que admita Private Link	Con las SKU admitidas de Azure Cognitive Search, Azure Private Link permite conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su servicio Search, se reduce el riesgo de pérdida de datos. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben deshabilitar el acceso a la red pública	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que se garantiza que el servicio de Azure Cognitive Search no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición del servicio Search. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la	Audit, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
usar un vínculo privado.	conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Cognitive Search, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azure-cognitive-search/inbound-private-endpoints.		
Las cuentas de Azure Cosmos DB deben tener reglas de firewall .	Se deben definir reglas de firewall en las cuentas de Azure Cosmos DB para evitar el tráfico desde orígenes no autorizados. Las cuentas que tienen al menos una regla de IP definida con el filtro de red virtual habilitado se consideran compatibles. Las cuentas que deshabilitan el acceso público también se consideran compatibles.	Audit, Deny, Disabled	2.0.0
Azure Data Factory debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Data Factory, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/data-factory/data-factory-private-link.	AuditIfNotExists, Disabled	1.0.0
Los dominios de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al dominio de Event Grid en lugar de a todo el servicio, también estará protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Los temas de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al tema de Event Grid en lugar de a todo el servicio, estará además protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure File Sync debe usar Private Link	Si crea un punto de conexión privado para el recurso del servicio de sincronización de almacenamiento indicado, podrá dirigirse al recurso del servicio de sincronización de almacenamiento desde el espacio de direcciones IP privadas de la red de la organización, en lugar de hacerlo a través del punto de conexión público accesible desde Internet. La creación de un punto de conexión privado por sí mismo no deshabilita el punto de conexión público.	AuditIfNotExists, Disabled	1.0.0
Azure Key Vault debe deshabilitar el acceso de red público.	Deshabilite el acceso de red público para el almacén de claves de modo que no sea accesible mediante la red pública de Internet. Esto puede reducir los riesgos de pérdida de datos. Más información en: https://aka.ms/akvprivatelink.	Audit, Deny, Disabled	2.0.0-preview
Las áreas de trabajo de Azure Machine Learning deben usar un vínculo privado .	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a áreas de trabajo de Azure Machine Learning, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link.	Audit, Deny, Disabled	1.1.0
Los espacios de nombres de Azure Service Bus deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres de Service Bus, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/service-bus-messaging/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Azure SignalR Service debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su recurso de Azure SignalR	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Service en lugar todo el servicio, reducirá los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/asrs/privatelink.		
Las áreas de trabajo de Azure Synapse deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al área de trabajo de Azure Synapse, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links.	Audit, Disabled	1.0.1
El servicio Azure Web PubSub debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su servicio Azure Web PubSub, puede reducir los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/awps/privatelink .	Audit, Deny, Disabled	1.0.0
Las cuentas de Cognitive Services deben deshabilitar el acceso a la red pública.	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que la cuenta de Cognitive Services no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición de la cuenta de Cognitive Services. Más información en: https://go.microsoft.com/fwlink/?linkid=2129800.	Audit, Deny, Disabled	2.0.0
Las cuentas de Cognitive Services deben restringir el acceso a la red	Se debe restringir el acceso de red a las cuentas de Cognitive Services. Configure reglas de red, de forma que solo las aplicaciones de redes permitidas pueden acceder a la cuenta de Cognitive Services. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	2.0.0
Cognitive Services debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al	Audit, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	asignar puntos de conexión privados a Cognitive Services, reducirá la posibilidad de pérdida de datos. Más información sobre los vínculos privados en https://go.microsoft.com/fwlink/?linkid=2129800.		
Las instancias de Container Registry no deben permitir el acceso de red sin restricciones	De manera predeterminada, las instancias de Azure Container Registry aceptan conexiones a través de Internet de hosts de cualquier red. Para protegerlas frente a posibles amenazas, permita el acceso solo desde direcciones IP públicas específicas o intervalos de direcciones. Si el registro no tiene una regla de IP/firewall o una red virtual configurada, aparece en los recursos incorrectos. Obtenga más información sobre las reglas de red de Container Registry aquí: https://aka.ms/acr/portal/public-network y aquí https://aka.ms/acr/vnet.	Audit, Deny, Disabled	1.1.0
Las instancias de Container Registry deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link controla la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a las instancias de Container Registry en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/acr/private-link.	Audit, Disabled	1.0.1
Las cuentas de CosmosDB deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de CosmosDB, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints.	Audit, Disabled	1.0.0
Los recursos de acceso al disco deben usar un vínculo privado	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a diskAccesses, se reduce el riesgo de pérdida de	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	datos. Más información sobre los vínculos privados en https://aka.ms/disksprivatelinksdoc.		
Los espacios de nombres del centro de eventos deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres del centro de eventos, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/event-hubs/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Las máquinas virtuales accesibles desde Internet deben estar protegidas con grupos de seguridad de red	Proteja sus máquinas virtuales de posibles amenazas limitando el acceso a ellas con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0
Las instancias del servicio de aprovisionamiento de dispositivos de IoT Hub deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al servicio de aprovisionamiento de dispositivos de IoT Hub, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/iotdpsvnet.	Audit, Disabled	1.0.0
El reenvío de IP en la máquina virtual debe estar deshabilitado	Habilitar el reenvío de IP en la NIC de la máquina virtual permite que la máquina reciba tráfico dirigido a otros destinos. El reenvío de IP rara vez es necesario (por ejemplo, cuando se usa la máquina virtual como una aplicación virtual de red) y, por lo tanto, el equipo de seguridad de red debe revisarlo.	AuditIfNotExists, Disabled	3.0.0
Los puertos de administración de las máquinas virtuales deben protegerse con el control	Azure Security Center supervisará el posible acceso de red Just-In-Time (JIT) como recomendaciones.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
de acceso de red Just-In-Time .			
Se deben cerrar los puertos de administración en las máquinas virtuales	Los puertos de administración remota abiertos exponen la máquina virtual a un alto nivel de riesgo de recibir ataques basados en Internet. Estos ataques intentan averiguar las credenciales por medio de fuerza bruta a fin de obtener acceso de administrador a la máquina	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1622: protección de límites	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1623: protección de límites	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1624: protección de límites	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Las máquinas virtuales sin conexión a Internet deben protegerse con grupos de seguridad de red	Proteja las máquinas virtuales no accesibles desde Internet de posibles amenazas limitando el acceso con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0
Las conexiones de punto de conexión privado en Azure SQL Database deben estar habilitadas	Las conexiones de punto de conexión privado garantizan una comunicación segura al habilitar la conectividad privada con Azure SQL Database.	Audit, Disabled	1.1.0
Se debe configurar un punto de conexión privado	Private Link proporciona una manera de conectar Key Vault a los recursos de Azure sin enviar tráfico a través de la red pública de Internet. Un vínculo privado proporciona	Audit, Deny, Disabled	1.1.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
para Key Vault	varios niveles de protección contra la filtración de datos.		
El punto de conexión privado debe estar habilitado para servidores MariaDB	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for MariaDB. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores MySQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada a Azure Database for MySQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores PostgreSQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for PostgreSQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
Debe deshabilitarse el acceso a redes públicas en Azure SQL Database	Al deshabilitar la propiedad de acceso a la red pública, se mejora la seguridad al garantizar que solo se pueda acceder a la instancia de Azure SQL Database desde un punto de conexión privado. Esta configuración deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o redes virtuales.	Audit, Deny, Disabled	1.1.0
El acceso a redes públicas debe estar deshabilitado para los servidores MariaDB	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MariaDB desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El acceso a las redes públicas debe estar deshabilitado para los servidores MySQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MySQL desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2
El acceso a redes públicas debe estar deshabilitado para los servidores PostgreSQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for PostgreSQL desde un punto de conexión privado. Esta configuración deshabilita el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coinciden con las reglas de firewall basadas en la IP o en la red virtual.	Audit, Disabled	1.0.2
No se debe permitir el acceso público a la cuenta de almacenamiento	El acceso de lectura público anónimo a contenedores y blobs de Azure Storage es una manera cómoda de compartir datos, pero también puede plantear riesgos para la seguridad. Para evitar las infracciones de datos producidas por el acceso anónimo no deseado, Microsoft recomienda impedir el acceso público a una cuenta de almacenamiento a menos que su escenario lo requiera.	deshabilitado	3.0.1-preview
Se debe restringir el acceso de red a las cuentas de almacenamiento	El acceso de red a las cuentas de almacenamiento debe estar restringido. Configure reglas de red, solo las aplicaciones de redes permitidas pueden acceder a la cuenta de almacenamiento. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	1.1.1
Las cuentas de almacenamiento deben restringir el acceso a la red mediante el uso de reglas de red virtual	Proteja las cuentas de almacenamiento frente a amenazas potenciales mediante reglas de red virtual como método preferente en lugar de filtrado basado en IP. La deshabilitación del filtrado basado en IP evita que las direcciones IP públicas accedan a las cuentas de almacenamiento.	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las cuentas de almacenamiento deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de almacenamiento, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azureprivatelinkoverview.	AuditIfNotExists, Disabled	2.0.0
Las subredes deben estar asociadas con un grupo de seguridad de red.	Proteja la subred de posibles amenazas mediante la restricción del acceso con un grupo de seguridad de red (NSG). Estos grupos contienen las reglas de la lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a la subred.	AuditIfNotExists, Disabled	3.0.0
Las plantillas de VM Image Builder deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los recursos de creación del generador de imágenes de máquina virtual, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet.	Audit, Disabled, Deny	1.1.0
El firewall de aplicaciones web (WAF) debe estar habilitado para Application Gateway	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.	Audit, Deny, Disabled	1.0.1
Web Application Firewall (WAF) debe estar	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
habilitado en el servicio Azure Front Door Service	vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.		

Puntos de acceso

Id. : NIST SP 800-53 Rev. 4 SC-7 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las recomendaciones de protección de red adaptable se deben aplicar en las máquinas virtuales accesibles desde Internet	Azure Security Center analiza los patrones de tráfico de máquinas virtuales orientadas a Internet y proporciona recomendaciones de reglas de grupo de seguridad de red que reducen la superficie de ataque potencial.	AuditIfNotExists, Disabled	3.0.0
Todo el tráfico de Internet debe enrutarse mediante la instancia de Azure Firewall implementada	Azure Security Center ha identificado que algunas de las subredes no están protegidas con un firewall de próxima generación. Proteja las subredes frente a posibles amenazas mediante la restricción del acceso a ellas con Azure Firewall o un firewall de próxima generación compatible.	AuditIfNotExists, Disabled	3.0.0-preview
Todos los puertos de red deben estar restringidos en los grupos de seguridad de red asociados a la máquina virtual	Azure Security Center identificó que algunas de las reglas de entrada de sus grupos de seguridad de red son demasiado permisivas. Las reglas de entrada no deben permitir el acceso desde los intervalos "Cualquiera" o "Internet". Esto podría permitir que los atacantes pudieran acceder a sus recursos.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los servicios de API Management deben usar una red virtual	La implementación de Azure Virtual Network ofrece una seguridad y aislamiento mejorados, y permite colocar el servicio de API Management en una red enrutable sin conexión a Internet cuyo acceso puede controlar. Estas redes se pueden conectar a las redes locales mediante diversas tecnologías de VPN, lo que permite el acceso a los servicios de back-end dentro de la red o de forma local. El portal para desarrolladores y la puerta de enlace de API pueden configurarse para que sea accesible desde Internet o solo dentro de la red virtual.	Audit, Disabled	1.0.1
App Configuration debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a las instancias de App Configuration en lugar de a todo el servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/appconfig/private-endpoint.	AuditIfNotExists, Disabled	1.0.2
Los intervalos IP autorizados deben definirse en los servicios de Kubernetes	Restrinja el acceso a la API de administración de servicios de Kubernetes mediante la concesión de acceso de API solo a direcciones IP en intervalos específicos. Se recomienda limitar el acceso a los intervalos IP autorizados para garantizar que solo las aplicaciones de las redes permitidas puedan acceder al clúster.	Audit, Disabled	2.0.1
Azure API for FHIR debe usar un vínculo privado.	Azure API for FHIR debe tener al menos una conexión de punto de conexión privado aprobada. Los clientes de una red virtual pueden acceder de forma segura a los recursos que tengan conexiones de punto de conexión privadas mediante vínculos privados. Para más información, visite https://aka.ms/fhir-privatelink.	Audit, Disabled	1.0.0
Azure Cache for Redis debe usar Private Link	Los puntos de conexión privados le permiten conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. Al asignar puntos de conexión privados a las instancias de Azure Cache for Redis, se reduce el riesgo de pérdida de datos. Más información en: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El servicio Azure Cognitive Search debe usar una SKU que admita Private Link	Con las SKU admitidas de Azure Cognitive Search, Azure Private Link permite conectar la red virtual a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su servicio Search, se reduce el riesgo de pérdida de datos. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben deshabilitar el acceso a la red pública	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que se garantiza que el servicio de Azure Cognitive Search no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición del servicio Search. Más información en: https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Deny, Disabled	1.0.0
Los servicios de Azure Cognitive Search deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Cognitive Search, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azure-cognitive-search/inbound-private-endpoints.	Audit, Disabled	1.0.0
Las cuentas de Azure Cosmos DB deben tener reglas de firewall .	Se deben definir reglas de firewall en las cuentas de Azure Cosmos DB para evitar el tráfico desde orígenes no autorizados. Las cuentas que tienen al menos una regla de IP definida con el filtro de red virtual habilitado se consideran compatibles. Las cuentas que deshabilitan el acceso público también se consideran compatibles.	Audit, Deny, Disabled	2.0.0
Azure Data Factory debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a Azure Data Factory, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/data-factory/data-factory-private-link.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los dominios de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al dominio de Event Grid en lugar de a todo el servicio, también estará protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Los temas de Azure Event Grid deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al tema de Event Grid en lugar de a todo el servicio, estará además protegido frente a riesgos de pérdida de datos. Más información en: https://aka.ms/privateendpoints.	Audit, Disabled	1.0.2
Azure File Sync debe usar Private Link	Si crea un punto de conexión privado para el recurso del servicio de sincronización de almacenamiento indicado, podrá dirigirse al recurso del servicio de sincronización de almacenamiento desde el espacio de direcciones IP privadas de la red de la organización, en lugar de hacerlo a través del punto de conexión público accesible desde Internet. La creación de un punto de conexión privado por sí mismo no deshabilita el punto de conexión público.	AuditIfNotExists, Disabled	1.0.0
Azure Key Vault debe deshabilitar el acceso de red público.	Deshabilite el acceso de red público para el almacén de claves de modo que no sea accesible mediante la red pública de Internet. Esto puede reducir los riesgos de pérdida de datos. Más información en: https://aka.ms/akvprivatelink.	Audit, Deny, Disabled	2.0.0-preview
Las áreas de trabajo de Azure Machine Learning deben usar un vínculo privado .	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a áreas de trabajo de Azure Machine Learning, se reducen los riesgos de pérdida de datos. Más información sobre	Audit, Deny, Disabled	1.1.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	los vínculos privados en https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link.		
Los espacios de nombres de Azure Service Bus deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres de Service Bus, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/service-bus-messaging/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Azure SignalR Service debe usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su recurso de Azure SignalR Service en lugar todo el servicio, reducirá los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/asrs/privatelink.	Audit, Deny, Disabled	1.0.1
Las áreas de trabajo de Azure Synapse deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al área de trabajo de Azure Synapse, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links.	Audit, Disabled	1.0.1
El servicio Azure Web PubSub debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a su servicio Azure Web PubSub, puede reducir los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/awps/privatelink .	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las cuentas de Cognitive Services deben deshabilitar el acceso a la red pública.	Al deshabilitar el acceso a la red pública, se mejora la seguridad, ya que la cuenta de Cognitive Services no se expone en la red pública de Internet. La creación de puntos de conexión privados puede limitar la exposición de la cuenta de Cognitive Services. Más información en: https://go.microsoft.com/fwlink/?linkid=2129800.	Audit, Deny, Disabled	2.0.0
Las cuentas de Cognitive Services deben restringir el acceso a la red	Se debe restringir el acceso de red a las cuentas de Cognitive Services. Configure reglas de red, de forma que solo las aplicaciones de redes permitidas pueden acceder a la cuenta de Cognitive Services. Para permitir conexiones desde clientes específicos locales o de Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.	Audit, Deny, Disabled	2.0.0
Cognitive Services debe usar un vínculo privado	Azure Private Link permite conectar las redes virtuales a los servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a Cognitive Services, reducirá la posibilidad de pérdida de datos. Más información sobre los vínculos privados en https://go.microsoft.com/fwlink/?linkid=2129800.	Audit, Disabled	2.0.0
Las instancias de Container Registry no deben permitir el acceso de red sin restricciones	De manera predeterminada, las instancias de Azure Container Registry aceptan conexiones a través de Internet de hosts de cualquier red. Para protegerlas frente a posibles amenazas, permita el acceso solo desde direcciones IP públicas específicas o intervalos de direcciones. Si el registro no tiene una regla de IP/firewall o una red virtual configurada, aparece en los recursos incorrectos. Obtenga más información sobre las reglas de red de Container Registry aquí: https://aka.ms/acr/portal/public-network y aquí https://aka.ms/acr/vnet.	Audit, Deny, Disabled	1.1.0
Las instancias de Container Registry deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link controla la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a las instancias de Container Registry en lugar de a todo el	Audit, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	servicio, además se protege frente a riesgos de pérdida de datos. Más información en: https://aka.ms/acr/private-link.		
Las cuentas de CosmosDB deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de CosmosDB, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints.	Audit, Disabled	1.0.0
Los recursos de acceso al disco deben usar un vínculo privado	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a diskAccesses, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/disksprivatelinksdoc.	AuditIfNotExists, Disabled	1.0.0
Los espacios de nombres del centro de eventos deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los espacios de nombres del centro de eventos, se reducen los riesgos de pérdida de datos. Más información en: https://docs.microsoft.com/azure/event-hubs/private-link-service.	AuditIfNotExists, Disabled	1.0.0
Las máquinas virtuales accesibles desde Internet deben estar protegidas con grupos de seguridad de red	Proteja sus máquinas virtuales de posibles amenazas limitando el acceso a ellas con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0
Las instancias del servicio de aprovisionamiento de	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la	Audit, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
dispositivos de IoT Hub deben usar Private Link	conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados al servicio de aprovisionamiento de dispositivos de IoT Hub, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/iotdpsvnet.		
El reenvío de IP en la máquina virtual debe estar deshabilitado	Habilitar el reenvío de IP en la NIC de la máquina virtual permite que la máquina reciba tráfico dirigido a otros destinos. El reenvío de IP rara vez es necesario (por ejemplo, cuando se usa la máquina virtual como una aplicación virtual de red) y, por lo tanto, el equipo de seguridad de red debe revisarlo.	AuditIfNotExists, Disabled	3.0.0
Los puertos de administración de las máquinas virtuales deben protegerse con el control de acceso de red Just-In-Time .	Azure Security Center supervisará el posible acceso de red Just-In-Time (JIT) como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
Se deben cerrar los puertos de administración en las máquinas virtuales	Los puertos de administración remota abiertos exponen la máquina virtual a un alto nivel de riesgo de recibir ataques basados en Internet. Estos ataques intentan averiguar las credenciales por medio de fuerza bruta a fin de obtener acceso de administrador a la máquina	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1625: protección de límites | Puntos de acceso	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Las máquinas virtuales sin conexión a Internet deben protegerse con grupos de seguridad de red	Proteja las máquinas virtuales no accesibles desde Internet de posibles amenazas limitando el acceso con grupos de seguridad de red (NSG). Más información sobre cómo controlar el tráfico con los grupos de seguridad de red en https://aka.ms/nsg-doc.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las conexiones de punto de conexión privado en Azure SQL Database deben estar habilitadas	Las conexiones de punto de conexión privado garantizan una comunicación segura al habilitar la conectividad privada con Azure SQL Database.	Audit, Disabled	1.1.0
Se debe configurar un punto de conexión privado para Key Vault	Private Link proporciona una manera de conectar Key Vault a los recursos de Azure sin enviar tráfico a través de la red pública de Internet. Un vínculo privado proporciona varios niveles de protección contra la filtración de datos.	Audit, Deny, Disabled	1.1.0-preview
El punto de conexión privado debe estar habilitado para servidores MariaDB	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for MariaDB. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores MySQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada a Azure Database for MySQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
El punto de conexión privado debe estar habilitado para servidores PostgreSQL	Las conexiones de punto de conexión privado garantizan una comunicación segura al permitir la conectividad privada con Azure Database for PostgreSQL. Configure una conexión de punto de conexión privado para permitir el acceso al tráfico que solo proviene de redes conocidas y evitar el acceso desde todas las demás direcciones IP, incluido desde Azure.	AuditIfNotExists, Disabled	1.0.2
Debe deshabilitarse el acceso a redes públicas en Azure SQL Database	Al deshabilitar la propiedad de acceso a la red pública, se mejora la seguridad al garantizar que solo se pueda acceder a la instancia de Azure SQL Database desde un punto de conexión privado. Esta configuración deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o redes virtuales.	Audit, Deny, Disabled	1.1.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El acceso a redes públicas debe estar deshabilitado para los servidores MariaDB	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MariaDB desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2
El acceso a las redes públicas debe estar deshabilitado para los servidores MySQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for MySQL desde un punto de conexión privado. Esta configuración deshabilita estrictamente el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coincidan con las reglas de firewall basadas en IP o en red virtual.	Audit, Disabled	1.0.2
El acceso a redes públicas debe estar deshabilitado para los servidores PostgreSQL	Deshabilite la propiedad de acceso a la red pública para mejorar la seguridad y garantizar que solo se pueda acceder a la instancia de Azure Database for PostgreSQL desde un punto de conexión privado. Esta configuración deshabilita el acceso desde cualquier espacio de direcciones público que esté fuera del intervalo de direcciones IP de Azure y deniega todos los inicios de sesión que coinciden con las reglas de firewall basadas en la IP o en la red virtual.	Audit, Disabled	1.0.2
No se debe permitir el acceso público a la cuenta de almacenamiento	El acceso de lectura público anónimo a contenedores y blobs de Azure Storage es una manera cómoda de compartir datos, pero también puede plantear riesgos para la seguridad. Para evitar las infracciones de datos producidas por el acceso anónimo no deseado, Microsoft recomienda impedir el acceso público a una cuenta de almacenamiento a menos que su escenario lo requiera.	deshabilitado	3.0.1-preview
Se debe restringir el acceso de red a las cuentas de almacenamiento	El acceso de red a las cuentas de almacenamiento debe estar restringido. Configure reglas de red, solo las aplicaciones de redes permitidas pueden acceder a la cuenta de almacenamiento. Para permitir conexiones desde clientes específicos locales o de	Audit, Deny, Disabled	1.1.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Internet, se puede conceder acceso al tráfico procedente de redes virtuales de Azure específicas o a intervalos de direcciones IP de Internet públicas.		
Las cuentas de almacenamiento deben restringir el acceso a la red mediante el uso de reglas de red virtual	Proteja las cuentas de almacenamiento frente a amenazas potenciales mediante reglas de red virtual como método preferente en lugar de filtrado basado en IP. La deshabilitación del filtrado basado en IP evita que las direcciones IP públicas accedan a las cuentas de almacenamiento.	Audit, Deny, Disabled	1.0.1
Las cuentas de almacenamiento deben usar un vínculo privado.	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Al asignar puntos de conexión privados a su cuenta de almacenamiento, se reduce el riesgo de pérdida de datos. Más información sobre los vínculos privados en https://aka.ms/azureprivatelinkoverview.	AuditIfNotExists, Disabled	2.0.0
Las subredes deben estar asociadas con un grupo de seguridad de red.	Proteja la subred de posibles amenazas mediante la restricción del acceso con un grupo de seguridad de red (NSG). Estos grupos contienen las reglas de la lista de control de acceso (ACL) que permiten o deniegan el tráfico de red a la subred.	AuditIfNotExists, Disabled	3.0.0
Las plantillas de VM Image Builder deben usar Private Link	Azure Private Link permite conectar la red virtual a servicios de Azure sin una dirección IP pública en el origen o el destino. La plataforma Private Link administra la conectividad entre el consumidor y los servicios a través de la red troncal de Azure. Mediante la asignación de puntos de conexión privados a los recursos de creación del generador de imágenes de máquina virtual, se reducen los riesgos de pérdida de datos. Más información sobre los vínculos privados en https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet.	Audit, Disabled, Deny	1.1.0
El firewall de aplicaciones web (WAF) debe estar	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
habilitado para Application Gateway	vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.		
Web Application Firewall (WAF) debe estar habilitado en el servicio Azure Front Door Service	Implemente Azure Web Application Firewall (WAF) delante de las aplicaciones web de acceso público para una inspección adicional del tráfico entrante. Web Application Firewall (WAF) ofrece una protección centralizada de las aplicaciones web frente a vulnerabilidades de seguridad comunes, como la inyección de SQL, el scripting entre sitios y las ejecuciones de archivos locales y remotas. También permite restringir el acceso a las aplicaciones web por países o regiones, intervalos de direcciones IP y otros parámetros http(s) por medio de reglas personalizadas.	Audit, Deny, Disabled	1.0.1

Servicios de telecomunicaciones externas

Id. : NIST SP 800-53 Rev. 4 SC-7 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1626: protección de límites | Servicios de telecomunicaciones externas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1627: protección de límites | Servicios de telecomunicaciones externas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1628: protección de límites | Servicios de telecomunicaciones externas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1629: protección de límites | Servicios de telecomunicaciones externas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1630: protección de límites | Servicios de telecomunicaciones externas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Denegar de forma predeterminada o permitir mediante una excepción

Id. : NIST SP 800-53 Rev. 4 SC-7 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1631: protección de límites | Denegar de forma predeterminada o permitir mediante una excepción	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Impedir tunelización dividida para dispositivos remotos

Id. : NIST SP 800-53 Rev. 4 SC-7 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1632: protección de límites | Impedir tunelización dividida para dispositivos remotos	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Enrutamiento del tráfico a servidores proxy autenticados

Id. : NIST SP 800-53 Rev. 4 SC-7 (8)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1633: protección de límites | Enrutamiento del tráfico a servidores proxy autenticados	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Impedir exfiltración no autorizada

Id. : NIST SP 800-53 Rev. 4 SC-7 (10)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1634: protección de límites | Impedir exfiltración no autorizada	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Protección basada en host

Id. : NIST SP 800-53 Rev. 4 SC-7 (12)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1635: protección de límites | Protección basada en host	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Aislamiento de herramientas de seguridad, mecanismos y componentes de soporte técnico

Id. : NIST SP 800-53 Rev. 4 SC-7 (13)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1636: protección de límites | Aislamiento de herramientas de seguridad, mecanismos y componentes de soporte técnico	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Error de seguridad

Id. : NIST SP 800-53 Rev. 4 SC-7 (18)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1637: protección de límites | Error de seguridad	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Aislamiento o segregación dinámicos

Id. : NIST SP 800-53 Rev. 4 SC-7 (20)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1638: protección de límites | Aislamiento o segregación dinámicos	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Aislamiento de los componentes del sistema de información

Id. : NIST SP 800-53 Rev. 4 SC-7 (21)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1639: protección de límites | Aislamiento de los componentes del sistema de información	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Integridad y confidencialidad de transmisión

Id. : NIST SP 800-53 Rev. 4 SC-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Acceso a API App solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los clústeres de Azure HDInsight deben usar el cifrado en tránsito para cifrar la comunicación entre	Los datos se pueden alterar durante la transmisión entre los nodos de clúster de Azure HDInsight. Al habilitar el cifrado en tránsito se solucionan los problemas de uso indebido y manipulación durante esta transmisión.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
los nodos del clúster de Azure HDInsight .			
Exigir una conexión SSL debe estar habilitado en los servidores de bases de datos MySQL	Azure Database for MySQL permite conectar el servidor de Azure Database for MySQL con aplicaciones cliente mediante Capa de sockets seguros (SSL). La aplicación de conexiones SSL entre el servidor de bases de datos y las aplicaciones cliente facilita la protección frente a ataques de tipo "Man in the middle" al cifrar el flujo de datos entre el servidor y la aplicación. Esta configuración exige que SSL esté siempre habilitado para el acceso al servidor de bases de datos.	Audit, Disabled	1.0.1
La aplicación de la conexión SSL debe estar habilitada para los servidores de base de datos PostgreSQL	Azure Database for PostgreSQL permite conectar el servidor de Azure Database for PostgreSQL a las aplicaciones cliente mediante la Capa de sockets seguros (SSL). La aplicación de conexiones SSL entre el servidor de bases de datos y las aplicaciones cliente facilita la protección frente a ataques de tipo "Man in the middle" al cifrar el flujo de datos entre el servidor y la aplicación. Esta configuración exige que SSL esté siempre habilitado para el acceso al servidor de bases de datos.	Audit, Disabled	1.0.1
Es necesario exigir FTPS en la aplicación de API	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Es necesario exigir FTPS en la aplicación de funciones	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Es necesario exigir FTPS en la aplicación web	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Acceso a Function App solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los clústeres de Kubernetes solo deben ser accesibles a través de HTTPS	El uso de HTTPS garantiza la autenticación y protege los datos en tránsito frente a ataques de intercepción de nivel de red. Esta funcionalidad está disponible actualmente con carácter general para Kubernetes Service (AKS) y en versión	deshabilitado	6.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para más información, visite https://aka.ms/kubepolicydoc		
Debe usarse la versión más reciente de TLS en la aplicación de API	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0
Debe usarse la versión más reciente de TLS en la aplicación de funciones	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0
Debe usarse la versión más reciente de TLS en la aplicación web	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0
Control administrado por Microsoft 1640: integridad y confidencialidad de transmisión	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Solo se deben habilitar las conexiones seguras a la instancia de Azure Cache for Redis .	Permite auditar la habilitación solo de conexiones a Azure Cache for Redis a través de SSL. El uso de conexiones seguras garantiza la autenticación entre el servidor y el servicio, y protege los datos en tránsito de ataques de nivel de red, como "man in-the-middle", interceptación y secuestro de sesión	Audit, Deny, Disabled	1.0.0
Se debe habilitar la transferencia segura a las cuentas de almacenamiento	Permite auditar el requisito de transferencia segura en la cuenta de almacenamiento. La transferencia segura es una opción que obliga a la cuenta de almacenamiento a aceptar solamente solicitudes de conexiones seguras (HTTPS). El uso de HTTPS garantiza la autenticación entre el servidor y el servicio, y protege los datos en tránsito de ataques de nivel de red, como los de tipo "Man in the middle", interceptación y secuestro de sesión	Audit, Deny, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Acceso a la aplicación web solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los servidores web de Windows deben estar configurados para usar protocolos de comunicación seguros	Para proteger la privacidad de la información que se comunica a través de Internet, los servidores web deben usar la versión más reciente del protocolo criptográfico estándar del sector, Seguridad de la capa de transporte (TLS). TLS protege las comunicaciones que se realizan a través de una red mediante el uso de certificados de seguridad para cifrar una conexión entre máquinas.	AuditIfNotExists, Disabled	3.0.0

Protección física criptográfica o alternativa

Id. : NIST SP 800-53 Rev. 4 SC-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Acceso a API App solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los clústeres de Azure HDInsight deben usar el cifrado en tránsito para cifrar la comunicación entre los nodos del clúster de Azure HDInsight .	Los datos se pueden alterar durante la transmisión entre los nodos de clúster de Azure HDInsight. Al habilitar el cifrado en tránsito se solucionan los problemas de uso indebido y manipulación durante esta transmisión.	Audit, Deny, Disabled	1.0.0
Exigir una conexión SSL debe estar habilitado en los servidores de bases de datos MySQL	Azure Database for MySQL permite conectar el servidor de Azure Database for MySQL con aplicaciones cliente mediante Capa de sockets seguros (SSL). La aplicación de conexiones SSL entre el servidor de bases de datos y las aplicaciones cliente facilita la protección frente a ataques de tipo "Man in the middle" al cifrar el	Audit, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	flujo de datos entre el servidor y la aplicación. Esta configuración exige que SSL esté siempre habilitado para el acceso al servidor de bases de datos.		
La aplicación de la conexión SSL debe estar habilitada para los servidores de base de datos PostgreSQL	Azure Database for PostgreSQL permite conectar el servidor de Azure Database for PostgreSQL a las aplicaciones cliente mediante la Capa de sockets seguros (SSL). La aplicación de conexiones SSL entre el servidor de bases de datos y las aplicaciones cliente facilita la protección frente a ataques de tipo "Man in the middle" al cifrar el flujo de datos entre el servidor y la aplicación. Esta configuración exige que SSL esté siempre habilitado para el acceso al servidor de bases de datos.	Audit, Disabled	1.0.1
Es necesario exigir FTPS en la aplicación de API	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Es necesario exigir FTPS en la aplicación de funciones	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Es necesario exigir FTPS en la aplicación web	Habilite el cumplimiento con FTPS para mejorar la seguridad.	AuditIfNotExists, Disabled	2.0.0
Acceso a Function App solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los clústeres de Kubernetes solo deben ser accesibles a través de HTTPS	El uso de HTTPS garantiza la autenticación y protege los datos en tránsito frente a ataques de intercepción de nivel de red. Esta funcionalidad está disponible actualmente con carácter general para Kubernetes Service (AKS) y en versión preliminar para el motor de AKS y Kubernetes con Azure Arc habilitado. Para más información, visite https://aka.ms/kubepolicydoc	deshabilitado	6.0.0
Debe usarse la versión más reciente de TLS en la aplicación de API	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe usarse la versión más reciente de TLS en la aplicación de funciones	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0
Debe usarse la versión más reciente de TLS en la aplicación web	Actualiza a la versión más reciente de TLS.	AuditIfNotExists, Disabled	1.0.0
Control administrado por Microsoft 1641: integridad y confidencialidad de la transmisión | Protección física criptográfica o alternativa	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Solo se deben habilitar las conexiones seguras a la instancia de Azure Cache for Redis .	Permite auditar la habilitación solo de conexiones a Azure Cache for Redis a través de SSL. El uso de conexiones seguras garantiza la autenticación entre el servidor y el servicio, y protege los datos en tránsito de ataques de nivel de red, como "man in-the-middle", interceptación y secuestro de sesión	Audit, Deny, Disabled	1.0.0
Se debe habilitar la transferencia segura a las cuentas de almacenamiento	Permite auditar el requisito de transferencia segura en la cuenta de almacenamiento. La transferencia segura es una opción que obliga a la cuenta de almacenamiento a aceptar solamente solicitudes de conexiones seguras (HTTPS). El uso de HTTPS garantiza la autenticación entre el servidor y el servicio, y protege los datos en tránsito de ataques de nivel de red, como los de tipo "Man in the middle", interceptación y secuestro de sesión	Audit, Deny, Disabled	2.0.0
Acceso a la aplicación web solo a través de HTTPS	El uso de HTTPS garantiza la autenticación del servicio y el servidor, y protege los datos en tránsito frente a ataques de intercepción de nivel de red.	Audit, Disabled	1.0.0
Los servidores web de Windows deben estar configurados para	Para proteger la privacidad de la información que se comunica a través de Internet, los servidores web deben usar la versión más reciente del protocolo criptográfico estándar del sector, Seguridad de la capa de transporte (TLS). TLS protege las	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
usar protocolos de comunicación seguros	comunicaciones que se realizan a través de una red mediante el uso de certificados de seguridad para cifrar una conexión entre máquinas.		

Desconexión de red

Id. : NIST SP 800-53 Rev. 4 SC-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1642: desconexión de red	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Establecimiento y administración de una clave criptográfica

Id. : NIST SP 800-53 Rev. 4 SC-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Azure API for FHIR debe usar una clave administrada por el cliente para cifrar los datos en reposo.	Use claves administradas por el cliente para controlar el cifrado en reposo de los datos almacenados en Azure API for FHIR cuando exista un requisito normativo o de cumplimiento. Las claves administradas por el cliente también proporcionan cifrado doble, ya que agregan una segunda capa de cifrado además de la capa predeterminada que se creó mediante las claves administradas por el servicio.	deshabilitado	1.0.1
Las cuentas de Azure Automation deben usar	Use claves administradas por el cliente para administrar el cifrado en reposo de sus cuentas de Azure Automation. De manera predeterminada, los datos del cliente se	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
claves administradas por el cliente para cifrar los datos en reposo .	cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en [https://aka.ms/automation-cmk](../../../../automation/automation-secure-asset-encryption.md#:~:text=Los recursos seguros de Azure Automation incluyen credenciales, certificados, conexiones, uso de claves administradas por Microsoft).		
La cuenta de Azure Batch debe usar claves administradas por el cliente para cifrar los datos	Use claves administradas por el cliente para administrar el cifrado en reposo de los datos de la cuenta de Batch. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/Batch-CMK .	Audit, Deny, Disabled	1.0.1
El grupo de contenedores de la instancia de Azure Container Instances debe usar una clave administrada por el cliente para el cifrado	Proteja los contenedores con mayor flexibilidad mediante el uso de claves administradas por el cliente. Cuando se especifica una clave administrada por el cliente, esa clave se usa para proteger y controlar el acceso a la clave que cifra los datos. El uso de claves administradas por el cliente proporciona funcionalidades adicionales para controlar la rotación de la clave de cifrado de claves o para borrar datos mediante criptografía.	Audit, Disabled, Deny	1.0.0
Las cuentas de Azure Cosmos DB deben usar claves administradas por el cliente para cifrar los datos en reposo	Use claves administradas por el cliente para administrar el cifrado en reposo de la instancia de Azure Cosmos DB. De manera predeterminada, los datos se cifran en reposo con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/cosmosdb-cmk.	deshabilitado	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los trabajos de Azure Data Box deben usar una clave administrada por el cliente para cifrar la contraseña de desbloqueo del dispositivo	Use una clave administrada por el cliente para controlar el cifrado de la contraseña de desbloqueo del dispositivo para Azure Data Box. Las claves administradas por el cliente también ayudan a administrar el acceso a la contraseña de desbloqueo del dispositivo por parte del servicio Data Box para preparar el dispositivo y copiar los datos de forma automatizada. Los datos del propio dispositivo ya están cifrados en reposo con el Estándar de cifrado avanzado cifrado de 256 bits y la contraseña de desbloqueo del dispositivo se cifra de forma predeterminada con una clave administrada por Microsoft.	Audit, Deny, Disabled	1.0.0
El cifrado en reposo de Azure Data Explorer debe usar una clave administrada por el cliente	Al habilitar el cifrado en reposo con una clave administrada por el cliente en el clúster de Azure Data Explorer, se proporciona un mayor control sobre la clave que usa el cifrado en reposo. Esta característica se suele aplicar a los clientes con requisitos de cumplimiento especiales y requiere un almacén de claves para administrar las claves.	Audit, Deny, Disabled	1.0.0
Las instancias de Azure Data Factory deben cifrarse con una clave administrada por el cliente .	Utilice claves administradas por el cliente (CMK) para administrar el cifrado en reposo de los datos de Azure Data Factory. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/adf-cmk.	Audit, Deny, Disabled	1.0.1
Los clústeres de Azure HDInsight deben usar claves administradas por el cliente para cifrar los datos en reposo	Utilice claves administradas por el cliente para administrar el cifrado en reposo de los clústeres de Azure HDInsight. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad	Audit, Deny, Disabled	1.0.1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/hdi.cmk.		
Los clústeres de Azure HDInsight deben usar el cifrado en el host para cifrar los datos en reposo .	La habilitación del cifrado en el host ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de la organización. Cuando se habilita el cifrado en el host, los datos almacenados en el host de máquina virtual se cifran en reposo y se transmiten cifrados al servido Storage.	Audit, Deny, Disabled	1.0.0
Las áreas de trabajo de Azure Machine Learning deben cifrarse con una clave administrada por el cliente .	Administre el cifrado en reposo de los datos del área de trabajo de Azure Machine Learning con claves administradas por el cliente. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/azureml-workspaces-cmk.	Audit, Deny, Disabled	1.0.3
Los clústeres de registros de Azure Monitor se deben cifrar con una clave administrada por el cliente	Cree un clúster de registros de Azure Monitor con cifrado de claves administradas por el cliente. De manera predeterminada, los datos de registro se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para satisfacer el cumplimiento normativo. La clave administrada por el cliente en Azure Monitor proporciona un mayor control sobre el acceso a los datos; consulte https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys.	deshabilitado	1.0.0
los almacenes de Azure Recovery Services deben usar claves administradas por el cliente para cifrar los	Use claves administradas por el cliente para administrar el cifrado en reposo de los datos de copia de seguridad. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure	Audit, Deny, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
datos de copia de seguridad	Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/AB-CmkEncryption.		
Los trabajos de Azure Stream Analytics deben usar claves administradas por el cliente para cifrar los datos	Use las claves administradas por el cliente cuando quiera almacenar de forma segura los recursos de datos privados y los metadatos de sus trabajos de Stream Analytics en la cuenta de almacenamiento. De esta forma, dispondrá de un control total sobre la forma en que se cifran los datos de Stream Analytics.	deshabilitado	1.0.0
Las áreas de trabajo de Azure Synapse deben usar claves administradas por el cliente para cifrar los datos en reposo	Use claves administradas por el cliente para controlar el cifrado en reposo de los datos almacenados en las áreas de trabajo de Azure Synapse. Las claves administradas por el cliente también proporcionan cifrado doble, ya que agregan una segunda capa de cifrado a partir del cifrado predeterminado que se creó mediante las claves administradas por el servicio.	Audit, Deny, Disabled	1.0.0
Bot Service se debe cifrar con una clave administrada por el cliente	Azure Bot Service cifra automáticamente el recurso para proteger sus datos y satisfacer los compromisos de cumplimiento y seguridad de la organización. De forma predeterminada, se usan claves de cifrado administradas por Microsoft. Para una mayor flexibilidad en la administración de claves o el control del acceso a su suscripción, seleccione claves administradas por el cliente, también conocidas como Bring your own key (BYOK). Más información acerca del cifrado de Azure Bot Service: https://docs.microsoft.com/azure/bot-service/bot-service-encryption.	deshabilitado	1.0.0
Los sistemas operativos y los discos de datos de los clústeres de Azure Kubernetes Service deben cifrarse mediante claves administradas por el cliente	El cifrado de los sistemas operativos y los discos de datos mediante claves administradas por el cliente proporciona más control y mayor flexibilidad para la administración de claves. Este es un requisito común de muchos estándares de cumplimiento normativo y del sector.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las cuentas de Cognitive Services deben habilitar el cifrado de datos con una clave administrada por el cliente .	Las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos almacenados en Cognitive Services con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Para más información sobre las claves administradas por el cliente, consulte https://go.microsoft.com/fwlink/?linkid=2121321.	Audit, Deny, Disabled	2.0.0
Los registros de contenedor deben cifrarse con una clave administrada por el cliente	Use claves administradas por el cliente para administrar el cifrado en reposo del contenido de los registros. De manera predeterminada, los datos se cifran en reposo con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/acr/CMK.	Audit, Deny, Disabled	1.1.2
Los espacios de nombres deben usar una clave administrada por el cliente para el cifrado	Azure Event Hubs admite la opción de cifrado de datos en reposo con claves administradas por Microsoft (predeterminada) o claves administradas por el cliente. La selección del cifrado de datos mediante claves administradas por el cliente le permite asignar, rotar, deshabilitar y revocar el acceso a las claves que el centro de eventos usará para cifrar los datos en el espacio de nombres. Tenga en cuenta que el centro de eventos solo admite el cifrado con claves administradas por el cliente para los espacios de nombres en clústeres dedicados.	Audit, Disabled	1.0.0
Las cuentas de HPC Cache deben usar la clave administrada por el cliente para el cifrado	Administre el cifrado en reposo de Azure HPC Cache con claves administradas por el cliente. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key	Audit, Disabled, Deny	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración.		
Los datos del servicio de aprovisionamiento de dispositivos de IoT Hub se deben cifrar con claves administradas por el cliente (CMK)	Use claves administradas por el cliente para administrar el cifrado en reposo del servicio de aprovisionamiento de dispositivos de IoT Hub. Los datos se cifran automáticamente en reposo con claves administradas por el servicio, pero las claves administradas por el cliente (CMK) suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las CMK permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Más información sobre el cifrado de CMK en https://aka.ms/dps/CMK.	Audit, Deny, Disabled	1.0.0-preview
El Entorno del servicio de integración de Logic Apps se debe cifrar con claves administradas por el cliente.	Realice la implementación en el Entorno del servicio de integración para administrar el cifrado en reposo de los datos de Logic Apps con claves administradas por el cliente. De manera predeterminada, los datos del cliente se cifran con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración.	Audit, Deny, Disabled	1.0.0
Los discos administrados deben tener un cifrado doble con las claves administradas por el cliente y la plataforma	Los clientes con datos confidenciales de alto nivel de seguridad que están preocupados por el riesgo asociado a cualquier algoritmo de cifrado, implementación o clave en peligro concretos pueden optar por una capa adicional de cifrado con un algoritmo o modo de cifrado diferente en el nivel de infraestructura mediante claves de cifrado administradas por la plataforma. Los conjuntos de cifrado de disco son necesarios para usar el cifrado doble. Obtenga más información en https://aka.ms/disks-doubleEncryption.	Audit, Deny, Disabled	1.0.0
Control administrado por Microsoft 1643: establecimiento y	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
administración de una clave criptográfica			
Los servidores MySQL deben usar claves administradas por el cliente para cifrar los datos en reposo.	Use claves administradas por el cliente para administrar el cifrado en reposo de los servidores MySQL. De manera predeterminada, los datos se cifran en reposo con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración.	AuditIfNotExists, Disabled	1.0.4
El SO y los discos de datos deben cifrarse con una clave administrada por el cliente	Use claves administradas por el cliente para administrar el cifrado en reposo del contenido de Managed Disks. De manera predeterminada, los datos se cifran en reposo con claves administradas por la plataforma, pero las claves administradas por el cliente suelen ser necesarias para cumplir los estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información en https://aka.ms/disks-cmk.	Audit, Deny, Disabled	2.0.0
Los servidores PostgreSQL deben usar claves administradas por el cliente para cifrar los datos en reposo.	Use claves administradas por el cliente para administrar el cifrado en reposo de los servidores PostgreSQL. De manera predeterminada, los datos se cifran en reposo con claves administradas por el servicio, pero las claves administradas por el cliente suelen ser necesarias para cumplir estándares de cumplimiento normativo. Las claves administradas por el cliente permiten cifrar los datos con una clave de Azure Key Vault creada por el usuario y propiedad de este. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración.	AuditIfNotExists, Disabled	1.0.4
Las consultas guardadas de Azure Monitor deben guardarse en la cuenta de almacenamiento del	Vincule la cuenta de almacenamiento al área de trabajo de Log Analytics para proteger las consultas guardadas con el cifrado de la cuenta de almacenamiento. Las claves administradas por el cliente suelen ser necesarias para satisfacer el cumplimiento normativo y para tener un mayor control sobre el acceso a las consultas	deshabilitado	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
cliente para el cifrado de registros	guardadas en Azure Monitor. Para más información sobre lo anterior, consulte https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal.		
Los espacios de nombres prémium de Service Bus deben usar una clave administrada por el cliente para el cifrado	Azure Service Bus permite cifrar los datos en reposo con claves administradas por Microsoft (opción predeterminada) o claves administradas por el cliente. Si decide cifrar los datos con claves administradas por el cliente, podrá asignar, rotar, deshabilitar y revocar el acceso a las claves que Service Bus utiliza para cifrar los datos en el espacio de nombres. Tenga en cuenta que Service Bus solo admite el cifrado con claves administradas por el cliente en los espacios de nombres prémium.	Audit, Disabled	1.0.0
[En desuso]: las instancias administradas de SQL deben usar claves administradas por el cliente para cifrar los datos en reposo	La implementación de Cifrado de datos transparente (TDE) con una clave propia proporciona una mayor transparencia y control sobre el protector de TDE, ofrece mayor seguridad con un servicio externo respaldado con HSM y permite la separación de tareas. Esta recomendación se aplica a las organizaciones con un requisito de cumplimiento relacionado.	AuditIfNotExists, Disabled	1.0.2-deprecated
Los servidores SQL deben usar claves administradas por el cliente para cifrar los datos en reposo	La implementación de Cifrado de datos transparente (TDE) con una clave propia proporciona una mayor transparencia y control sobre el protector de TDE, ofrece mayor seguridad con un servicio externo respaldado con HSM y permite la separación de tareas. Esta recomendación se aplica a las organizaciones con un requisito de cumplimiento relacionado.	AuditIfNotExists, Disabled	2.0.1
Los ámbitos de cifrado de la cuenta de almacenamiento deben usar claves administradas por el cliente para cifrar los datos en reposo.	Use claves administradas por el cliente para administrar el cifrado en reposo de los ámbitos de cifrado de su cuenta de almacenamiento. Las claves administradas por el cliente le permiten cifrar los datos con una clave de Azure Key Vault que haya creado y sea de su propiedad. Tiene control y responsabilidad totales del ciclo de vida de la clave, incluidos la rotación y administración. Obtenga más información sobre los ámbitos de cifrado de la cuenta de almacenamiento en https://aka.ms/encryption-scopes-overview.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las cuentas de almacenamiento deben utilizar una clave administrada por el cliente para el cifrado	Proteja su cuenta de almacenamiento de blobs y archivos con mayor flexibilidad mediante claves administradas por el cliente. Cuando se especifica una clave administrada por el cliente, esa clave se usa para proteger y controlar el acceso a la clave que cifra los datos. El uso de claves administradas por el cliente proporciona funcionalidades adicionales para controlar la rotación de la clave de cifrado de claves o para borrar datos mediante criptografía.	Audit, Disabled	1.0.3

Disponibilidad

Id. : NIST SP 800-53 Rev. 4 SC-12 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1644: establecimiento y administración de una clave criptográfica | Disponibilidad	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Claves simétricas

Id. : NIST SP 800-53 Rev. 4 SC-12 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1645: establecimiento y administración de una clave criptográfica | Claves simétricas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Claves asimétricas

Id. : NIST SP 800-53 Rev. 4 SC-12 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1646: establecimiento y administración de una clave criptográfica | Claves asimétricas	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Protección criptográfica

Id. : NIST SP 800-53 Rev. 4 SC-13

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1647: protección criptográfica	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Dispositivos informáticos de colaboración

Id. : NIST SP 800-53 Rev. 4 SC-15

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1648: dispositivos informáticos de colaboración	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1649: dispositivos informáticos de colaboración	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Certificados de infraestructura de clave pública

Id. : NIST SP 800-53 Rev. 4 SC-17

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1650: certificados de infraestructura de clave pública	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Código móvil

Id. : NIST SP 800-53 Rev. 4 SC-18

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1651: código móvil	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1652: código móvil	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1653: código móvil	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Voz sobre IP (VoIP)

Id. : NIST SP 800-53 Rev. 4 SC-19

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1654: protocolo de voz sobre IP	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Control administrado por Microsoft 1655: protocolo de voz sobre IP	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Servicio de resolución de direcciones nombres seguro (origen de autoridad)

Id. : NIST SP 800-53 Rev. 4 SC-20

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1656: servicio seguro de resolución de direcciones y nombres (origen de autoridad)	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1657: servicio seguro de resolución de direcciones y nombres (origen de autoridad)	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Servicio de resolución de direcciones o nombres seguro (resolución recursiva o en caché)

Id. : NIST SP 800-53 Rev. 4 SC-21

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1657: servicio seguro de resolución de direcciones y nombres (resolución recursiva o en caché)	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Arquitectura y aprovisionamiento para el servicio de resolución de direcciones/nombres

Id. : NIST SP 800-53 Rev. 4 SC-22

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1659: arquitectura y aprovisionamiento para el servicio de resolución de direcciones y nombres	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Autenticidad de sesión

Id. : NIST SP 800-53 Rev. 4 SC-23

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1660: autenticidad de la sesión	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Invalidación de los identificadores de sesión al cerrar sesión

Id. : NIST SP 800-53 Rev. 4 SC-23 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1661: autenticidad de la sesión | Invalidación de los identificadores de sesión al cerrar sesión	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Error en estado conocido

Id. : NIST SP 800-53 Rev. 4 SC-24

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1662: error en estado conocido	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0

Protección de la información en reposo

Id. : NIST SP 800-53 Rev. 4 SC-28

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
App Service Environment debe habilitar el cifrado interno	Al establecer InternalEncryption en true, se cifra el archivo de paginación, los discos de trabajo y el tráfico de red interno entre los servidores front-end y los trabajos de una instancia de App Service Environment. Para más información, consulte https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption.	Audit, Disabled	1.0.0
Las variables de cuenta de Automation deben cifrarse	Es importante habilitar el cifrado de recursos de variables de cuentas de Automation al almacenar datos confidenciales.	Audit, Deny, Disabled	1.1.0
Los trabajos de Azure Data Box deben habilitar el cifrado doble para los datos en reposo en el dispositivo	Habilite una segunda capa de cifrado basado en software para los datos en reposo en el dispositivo. El dispositivo ya está protegido mediante el Estándar de cifrado avanzado de 256 bits para datos en reposo. Esta opción agrega una segunda capa de cifrado de datos.	Audit, Deny, Disabled	1.0.0
Los clústeres de registros de Azure Monitor se deben crear con el cifrado de infraestructura habilitado (cifrado doble)	Para asegurarse de que el cifrado de datos seguro está habilitado en el nivel de servicio y en el nivel de infraestructura con dos algoritmos de cifrado diferentes y dos claves diferentes, use un clúster dedicado Azure Monitor. Esta opción está habilitada de forma predeterminada cuando se admite en la región; consulte https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview.	deshabilitado	1.0.0
Los dispositivos Azure Stack Edge deben usar cifrado doble	Para proteger los datos en reposo del dispositivo, asegúrese de que tienen cifrado doble, se controla el acceso a ellos y, una vez desactivado el dispositivo, se borran de los discos de datos de forma segura. El cifrado doble consiste en dos capas de cifrado: XTS-AES de BitLocker de 256 bits en los volúmenes de datos y cifrado	deshabilitado	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	integrado en los discos duros. Más información en la documentación de información general sobre seguridad del dispositivo Stark Edge en cuestión.		
El cifrado de disco debe estar habilitado en Azure Data Explorer	La habilitación del cifrado de disco ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de la organización.	Audit, Deny, Disabled	2.0.0
El cifrado doble debe estar habilitado en Azure Data Explorer	La habilitación del cifrado doble ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de la organización. Cuando está habilitado el cifrado doble, los datos de las cuentas de almacenamiento se cifran dos veces, una vez en el nivel de servicio y otra en el nivel de infraestructura, con dos algoritmos de cifrado y dos claves diferentes.	Audit, Deny, Disabled	2.0.0
El cifrado de infraestructura debe estar habilitado para los servidores de Azure Database for MySQL	Habilite el cifrado de infraestructura para que los servidores de Azure Database for MySQL tengan mayor garantía de que los datos están seguros. Cuando se habilita el cifrado de infraestructura, los datos en reposo se cifran dos veces con las claves administradas de Microsoft compatibles con FIPS 140-2.	Audit, Deny, Disabled	1.0.0
El cifrado de infraestructura debe estar habilitado para los servidores de Azure Database for PostgreSQL	Habilite el cifrado de infraestructura para que los servidores de Azure Database for PostgreSQL tengan mayor garantía de que los datos están seguros. Cuando se habilita el cifrado de infraestructura, los datos en reposo se cifran dos veces con las claves administradas por Microsoft compatibles con FIPS 140-2.	Audit, Deny, Disabled	1.0.0
Control administrado por Microsoft 1663: protección de la información en reposo	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Los datos confidenciales de las bases de datos SQL deben clasificarse .	Azure Security Center supervisa los resultados del examen de clasificación y detección de los datos de las bases de datos SQL y proporciona recomendaciones para clasificar los datos confidenciales en las bases de datos y así poder mejorar los procesos de supervisión y la seguridad.	AuditIfNotExists, Disabled	3.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe establecer la propiedad ClusterProtectionLevel en EncryptAndSign en los clústeres de Service Fabric	Service Fabric proporciona tres niveles de protección (None, Sign y EncryptAndSign) para la comunicación de nodo a nodo mediante un certificado de clúster principal. Establezca el nivel de protección para asegurarse de que todos los mensajes de nodo a nodo se cifran y se firman digitalmente.	Audit, Deny, Disabled	1.1.0
Las cuentas de almacenamiento deben tener un cifrado de infraestructura	Habilite el cifrado de la infraestructura para aumentar la garantía de que los datos son seguros. Cuando el cifrado de infraestructura está habilitado, los datos de las cuentas de almacenamiento se cifran dos veces.	Audit, Deny, Disabled	1.0.0
Los discos temporales y la memoria caché de los grupos de nodos agente en los clústeres de Azure Kubernetes Service deben cifrarse en el host	Para mejorar la seguridad de los datos, los datos almacenados en el host de las máquinas virtuales de los nodos de Azure Kubernetes Service deben cifrarse en reposo. Este es un requisito común de muchos estándares de cumplimiento normativo y del sector.	Audit, Deny, Disabled	1.0.0
El cifrado de datos transparente en bases de datos SQL debe estar habilitado	El cifrado de datos transparente debe estar habilitado para proteger los datos en reposo y satisfacer los requisitos de cumplimiento.	AuditIfNotExists, Disabled	2.0.0
Las máquinas virtuales y los conjuntos de escalado de máquinas virtuales deben tener habilitado el cifrado en el host	Use el cifrado en el host para obtener el cifrado de un extremo a otro para la máquina virtual y los datos del conjunto de escalado de máquinas virtuales. El cifrado en el host permite el cifrado en reposo para las memorias caché de disco temporal y de sistema operativo y de datos. Los discos temporales y los discos de SO efímeros se cifran con claves administradas por la plataforma cuando se habilita el cifrado en el host. Las memorias caché del disco de datos y de sistema operativo se cifran en reposo con claves administradas por el cliente o por la plataforma, según el tipo de cifrado seleccionado en el disco. Obtenga más información en https://aka.ms/vm-hbe.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Las máquinas virtuales deben cifrar los discos temporales, las cachés y los flujos de datos entre los recursos de Proceso y Almacenamiento	De manera predeterminada, los discos del sistema operativo y de datos de una máquina virtual se cifran en reposo mediante claves administradas por la plataforma. Los discos temporales, las memorias caché de datos y los datos que fluyen entre el proceso y el almacenamiento no se cifran. Ignore esta recomendación si: 1. Se utiliza el cifrado en el host, o 2. El cifrado del lado servidor en Managed Disks cumple sus requisitos de seguridad. Más información en Cifrado del lado servidor de Azure Disk Storage y Diferentes ofertas de cifrado de disco.	AuditIfNotExists, Disabled	2.0.2

Protección criptográfica

Id. : NIST SP 800-53 Rev. 4 SC-28 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
App Service Environment debe habilitar el cifrado interno	Al establecer InternalEncryption en true, se cifra el archivo de paginación, los discos de trabajo y el tráfico de red interno entre los servidores front-end y los trabajos de una instancia de App Service Environment. Para más información, consulte https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption.	Audit, Disabled	1.0.0
Las variables de cuenta de Automation deben cifrarse	Es importante habilitar el cifrado de recursos de variables de cuentas de Automation al almacenar datos confidenciales.	Audit, Deny, Disabled	1.1.0
Los trabajos de Azure Data Box deben habilitar el cifrado doble para los datos en reposo en el dispositivo	Habilite una segunda capa de cifrado basado en software para los datos en reposo en el dispositivo. El dispositivo ya está protegido mediante el Estándar de cifrado avanzado de 256 bits para datos en reposo. Esta opción agrega una segunda capa de cifrado de datos.	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Los clústeres de registros de Azure Monitor se deben crear con el cifrado de infraestructura habilitado (cifrado doble)	Para asegurarse de que el cifrado de datos seguro está habilitado en el nivel de servicio y en el nivel de infraestructura con dos algoritmos de cifrado diferentes y dos claves diferentes, use un clúster dedicado Azure Monitor. Esta opción está habilitada de forma predeterminada cuando se admite en la región; consulte https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview.	deshabilitado	1.0.0
Los dispositivos Azure Stack Edge deben usar cifrado doble	Para proteger los datos en reposo del dispositivo, asegúrese de que tienen cifrado doble, se controla el acceso a ellos y, una vez desactivado el dispositivo, se borran de los discos de datos de forma segura. El cifrado doble consiste en dos capas de cifrado: XTS-AES de BitLocker de 256 bits en los volúmenes de datos y cifrado integrado en los discos duros. Más información en la documentación de información general sobre seguridad del dispositivo Stark Edge en cuestión.	deshabilitado	1.0.0
El cifrado de disco debe estar habilitado en Azure Data Explorer	La habilitación del cifrado de disco ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de la organización.	Audit, Deny, Disabled	2.0.0
El cifrado doble debe estar habilitado en Azure Data Explorer	La habilitación del cifrado doble ayuda a custodiar y proteger sus datos con el fin de satisfacer los compromisos de cumplimiento y seguridad de la organización. Cuando está habilitado el cifrado doble, los datos de las cuentas de almacenamiento se cifran dos veces, una vez en el nivel de servicio y otra en el nivel de infraestructura, con dos algoritmos de cifrado y dos claves diferentes.	Audit, Deny, Disabled	2.0.0
El cifrado de infraestructura debe estar habilitado para los servidores de Azure Database for MySQL	Habilite el cifrado de infraestructura para que los servidores de Azure Database for MySQL tengan mayor garantía de que los datos están seguros. Cuando se habilita el cifrado de infraestructura, los datos en reposo se cifran dos veces con las claves administradas de Microsoft compatibles con FIPS 140-2.	Audit, Deny, Disabled	1.0.0
El cifrado de infraestructura debe estar habilitado para los	Habilite el cifrado de infraestructura para que los servidores de Azure Database for PostgreSQL tengan mayor garantía de que los datos están seguros. Cuando se	Audit, Deny, Disabled	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
servidores de Azure Database for PostgreSQL	habilita el cifrado de infraestructura, los datos en reposo se cifran dos veces con las claves administradas por Microsoft compatibles con FIPS 140-2.		
Control administrado por Microsoft 1664: protección de la información en reposo | Protección criptográfica	Microsoft implementa este control de protección del sistema y de las comunicaciones	auditoría	1.0.0
Los datos confidenciales de las bases de datos SQL deben clasificarse .	Azure Security Center supervisa los resultados del examen de clasificación y detección de los datos de las bases de datos SQL y proporciona recomendaciones para clasificar los datos confidenciales en las bases de datos y así poder mejorar los procesos de supervisión y la seguridad.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe establecer la propiedad ClusterProtectionLevel en EncryptAndSign en los clústeres de Service Fabric	Service Fabric proporciona tres niveles de protección (None, Sign y EncryptAndSign) para la comunicación de nodo a nodo mediante un certificado de clúster principal. Establezca el nivel de protección para asegurarse de que todos los mensajes de nodo a nodo se cifran y se firman digitalmente.	Audit, Deny, Disabled	1.1.0
Las cuentas de almacenamiento deben tener un cifrado de infraestructura	Habilite el cifrado de la infraestructura para aumentar la garantía de que los datos son seguros. Cuando el cifrado de infraestructura está habilitado, los datos de las cuentas de almacenamiento se cifran dos veces.	Audit, Deny, Disabled	1.0.0
Los discos temporales y la memoria caché de los grupos de nodos agente en los clústeres de Azure Kubernetes Service deben cifrarse en el host	Para mejorar la seguridad de los datos, los datos almacenados en el host de las máquinas virtuales de los nodos de Azure Kubernetes Service deben cifrarse en reposo. Este es un requisito común de muchos estándares de cumplimiento normativo y del sector.	Audit, Deny, Disabled	1.0.0
El cifrado de datos transparente en bases de	El cifrado de datos transparente debe estar habilitado para proteger los datos en reposo y satisfacer los requisitos de cumplimiento.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
datos SQL debe estar habilitado			
Las máquinas virtuales y los conjuntos de escalado de máquinas virtuales deben tener habilitado el cifrado en el host	Use el cifrado en el host para obtener el cifrado de un extremo a otro para la máquina virtual y los datos del conjunto de escalado de máquinas virtuales. El cifrado en el host permite el cifrado en reposo para las memorias caché de disco temporal y de sistema operativo y de datos. Los discos temporales y los discos de SO efímeros se cifran con claves administradas por la plataforma cuando se habilita el cifrado en el host. Las memorias caché del disco de datos y de sistema operativo se cifran en reposo con claves administradas por el cliente o por la plataforma, según el tipo de cifrado seleccionado en el disco. Obtenga más información en https://aka.ms/vm-hbe.	Audit, Deny, Disabled	1.0.0
Las máquinas virtuales deben cifrar los discos temporales, las cachés y los flujos de datos entre los recursos de Proceso y Almacenamiento	De manera predeterminada, los discos del sistema operativo y de datos de una máquina virtual se cifran en reposo mediante claves administradas por la plataforma. Los discos temporales, las memorias caché de datos y los datos que fluyen entre el proceso y el almacenamiento no se cifran. Ignore esta recomendación si: 1. Se utiliza el cifrado en el host, o 2. El cifrado del lado servidor en Managed Disks cumple sus requisitos de seguridad. Más información en Cifrado del lado servidor de Azure Disk Storage y Diferentes ofertas de cifrado de disco.	AuditIfNotExists, Disabled	2.0.2

Aislamiento de procesos

Id. : NIST SP 800-53 Rev. 4 SC-39

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1665: aislamiento	Microsoft implementa este control de protección del sistema y de las	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
de procesos	comunicaciones		

Integridad del sistema y de la información

Procedimientos y directiva de integridad de la información y el sistema

Id. : NIST SP 800-53 Rev. 4 SI-1

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1666: procedimientos y directiva de integridad de la información y el sistema	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1667: procedimientos y directiva de integridad de la información y el sistema	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Corrección de errores

Id. : NIST SP 800-53 Rev. 4 SI-2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Debe habilitarse una solución de evaluación de	Audita las máquinas virtuales para detectar si ejecutan una solución de evaluación de vulnerabilidades admitida. Un componente fundamental de cada programa de	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
vulnerabilidades en sus máquinas virtuales	seguridad y riesgo cibernético es la identificación y el análisis de las vulnerabilidades. El plan de tarifa estándar de Azure Security Center incluye el análisis de vulnerabilidades de las máquinas virtuales sin costo adicional. Además, Security Center puede implementar automáticamente esta herramienta.		
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0-preview
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores SQL Server en las máquinas	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
Asegurarse de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Asegúrese de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegurarse de que la "Versión de Java" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de Java. Para las aplicaciones de API, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la versión de Java sea la más reciente, si se usa como parte de la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Java. Para las aplicaciones de funciones, se recomienda usar la versión más reciente de Java con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la "Versión de Java" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Java. Para las aplicaciones web, se recomienda usar la versión más reciente de Java con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.		
Asegurarse de que la "Versión de PHP" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de PHP. Para las aplicaciones de API, se recomienda usar la versión más reciente de PHP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.1.0
Asegúrese de que la "Versión de PHP" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de PHP. Para las aplicaciones web, se recomienda usar la versión más reciente de PHP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.1.0
Asegurarse de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones de API, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0
Asegúrese de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones de funciones, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Asegúrese de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones web, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0
Kubernetes Services se debe actualizar a una versión de Kubernetes no vulnerable	Actualice el clúster de servicio de Kubernetes a una versión de Kubernetes posterior para protegerse frente a vulnerabilidades conocidas en la versión actual de Kubernetes. La vulnerabilidad CVE-2019-9946 se ha revisado en las versiones de Kubernetes 1.11.9+, 1.12.7+, 1.13.5+ y 1.14.0+	Audit, Disabled	1.0.2
Control administrado por Microsoft 1668: corrección de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1669: corrección de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1670: corrección de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1671: corrección de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Las bases de datos SQL deben tener resueltos los hallazgos de vulnerabilidades.	Permite supervisar los resultados del examen de evaluación de puntos vulnerables y las recomendaciones para solucionar los de las bases de datos.	AuditIfNotExists, Disabled	4.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se deben instalar las actualizaciones del sistema en los conjuntos de escalado de máquinas virtuales	Audite si falta alguna actualización de seguridad del sistema o actualización crítica que deba instalarse para garantizar que los conjuntos de escalado de máquinas virtuales Windows y Linux sean seguros.	AuditIfNotExists, Disabled	3.0.0
Se deben instalar actualizaciones del sistema en las máquinas	Azure Security Center supervisará las actualizaciones del sistema de seguridad que faltan en los servidores como recomendaciones.	AuditIfNotExists, Disabled	4.0.0
Se deben corregir las vulnerabilidades en la configuración de seguridad en las máquinas	Azure Security Center supervisará los servidores que no cumplan la línea de base configurada como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
Se deben corregir las vulnerabilidades en la configuración de seguridad de los conjuntos de escalado de máquinas virtuales	Audite las vulnerabilidades del sistema operativo en los conjuntos de escalado de máquinas virtuales para protegerlos frente a ataques.	AuditIfNotExists, Disabled	3.0.0

Administración central

Id. : NIST SP 800-53 Rev. 4 SI-2 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1672: corrección de errores | Administración central	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Estado de corrección de errores automatizado

Id. : NIST SP 800-53 Rev. 4 SI-2 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1673: corrección de errores | Estado de corrección de errores automatizado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Tiempo para corregir errores o puntos de referencia para acciones correctivas

Id. : NIST SP 800-53 Rev. 4 SI-2 (3)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1674: corrección de errores | Tiempo para corregir errores o puntos de referencia para acciones correctivas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1675: corrección de errores | Tiempo para corregir errores o puntos de referencia para acciones correctivas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Eliminación de versiones anteriores de software o firmware

Id. : NIST SP 800-53 Rev. 4 SI-2 (6)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Asegurarse de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la "Versión de HTTP" es la más reciente, si se usa para ejecutar la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de HTTP. Para las aplicaciones web, use la versión más reciente de HTTP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegurarse de que la "Versión de Java" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes de Java. Para las aplicaciones de API, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegúrese de que la versión de Java sea la más reciente, si se usa como parte de la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Java. Para las aplicaciones de funciones, se recomienda usar la versión más reciente de Java con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Asegúrese de que la "Versión de Java" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Java. Para las aplicaciones web, se recomienda usar la versión más reciente de Java con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.0.0
Asegurarse de que la "Versión de PHP" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de PHP. Para las aplicaciones de API, se recomienda usar la versión más reciente de PHP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.1.0
Asegúrese de que la "Versión de PHP" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de PHP. Para las aplicaciones web, se recomienda usar la versión más reciente de PHP con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	2.1.0
Asegurarse de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación de API	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones de API, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0
Asegúrese de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación de funciones	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones de funciones, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Asegúrese de que la "Versión de Python" es la más reciente, si se usa como parte de la aplicación web	A causa de errores de seguridad o para incluir funcionalidades, se publican de forma periódica versiones más recientes del software de Python. Para las aplicaciones web, se recomienda usar la versión más reciente de Python con el fin de aprovechar las correcciones de seguridad, de haberlas, o las nuevas funcionalidades de la versión más reciente. Actualmente, esta directiva solo se aplica a las aplicaciones web de Linux.	AuditIfNotExists, Disabled	3.0.0
Kubernetes Services se debe actualizar a una versión de Kubernetes no vulnerable	Actualice el clúster de servicio de Kubernetes a una versión de Kubernetes posterior para protegerse frente a vulnerabilidades conocidas en la versión actual de Kubernetes. La vulnerabilidad CVE-2019-9946 se ha revisado en las versiones de Kubernetes 1.11.9+, 1.12.7+, 1.13.5+ y 1.14.0+	Audit, Disabled	1.0.2

Protección frente a código malintencionado

Id. : NIST SP 800-53 Rev. 4 SI-3

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
La solución de protección del punto de conexión debe instalarse en las máquinas virtuales	Audite la existencia y el estado de una solución de protección de puntos de conexión en los conjuntos de escalado de máquinas virtuales para protegerlos frente a amenazas y vulnerabilidades.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1676: protección	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
frente a código malintencionado			
Control administrado por Microsoft 1677: protección frente a código malintencionado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1678: protección frente a código malintencionado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1679: protección frente a código malintencionado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Supervisar la falta de Endpoint Protection en Azure Security Center	Azure Security Center supervisará los servidores sin un agente de Endpoint Protection instalado como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
La Protección contra vulnerabilidades de seguridad de Windows Defender debe estar habilitada en las máquinas .	La protección contra vulnerabilidades de seguridad de Windows Defender utiliza el agente de configuración de invitado de Azure Policy. La protección contra vulnerabilidades de seguridad tiene cuatro componentes diseñados para bloquear dispositivos en una amplia variedad de vectores de ataque y comportamientos de bloque utilizados habitualmente en ataques de malware, al tiempo que permiten a las empresas equilibrar los requisitos de productividad y riesgo de seguridad (solo Windows).	AuditIfNotExists, Disabled	1.1.1

Administración central

Id. : NIST SP 800-53 Rev. 4 SI-3 (1)

Nombre (Azure Portal)	**Descripción**	**Efectos**	**Versión** (GitHub)
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
La solución de protección del punto de conexión debe instalarse en las máquinas virtuales	Audite la existencia y el estado de una solución de protección de puntos de conexión en los conjuntos de escalado de máquinas virtuales para protegerlos frente a amenazas y vulnerabilidades.	AuditIfNotExists, Disabled	3.0.0
Control administrado por Microsoft 1680: protección frente a código malintencionado | Administración central	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Supervisar la falta de Endpoint Protection en Azure Security Center	Azure Security Center supervisará los servidores sin un agente de Endpoint Protection instalado como recomendaciones.	AuditIfNotExists, Disabled	3.0.0
La Protección contra vulnerabilidades de seguridad de Windows Defender debe estar habilitada en las máquinas .	La protección contra vulnerabilidades de seguridad de Windows Defender utiliza el agente de configuración de invitado de Azure Policy. La protección contra vulnerabilidades de seguridad tiene cuatro componentes diseñados para bloquear dispositivos en una amplia variedad de vectores de ataque y comportamientos de bloque utilizados habitualmente en ataques de malware, al tiempo que permiten a las empresas equilibrar los requisitos de productividad y riesgo de seguridad (solo Windows).	AuditIfNotExists, Disabled	1.1.1

Actualizaciones automáticas

Id. : NIST SP 800-53 Rev. 4 SI-3 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1681: protección frente a código malintencionado | Actualizaciones automáticas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Detección no basada en firmas

Id. : NIST SP 800-53 Rev. 4 SI-3 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1682: protección frente a código malintencionado | Detección no basada en firmas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Supervisión del sistema de información

Id. : NIST SP 800-53 Rev. 4 SI-4

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Todo el tráfico de Internet debe enrutarse mediante la	Azure Security Center ha identificado que algunas de las subredes no están protegidas con un firewall de próxima generación. Proteja las subredes frente a posibles amenazas	AuditIfNotExists, Disabled	3.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
instancia de Azure Firewall implementada	mediante la restricción del acceso a ellas con Azure Firewall o un firewall de próxima generación compatible.		
El aprovisionamiento automático del agente de Log Analytics debe estar habilitado en la suscripción	A fin de supervisar las amenazas y vulnerabilidades de seguridad, Azure Security Center recopila datos de las máquinas virtuales de Azure. El agente de Log Analytics, anteriormente conocido como Microsoft Monitoring Agent (MMA), recopila los datos al leer distintas configuraciones relacionadas con la seguridad y distintos registros de eventos de la máquina y copiar los datos en el área de trabajo de Log Analytics para analizarlos. Se recomienda habilitar el aprovisionamiento automático para implementar automáticamente el agente en todas las máquinas virtuales de Azure admitidas y en las nuevas que se creen.	AuditIfNotExists, Disabled	1.0.1
Los clústeres de Kubernetes habilitados para Azure Arc deben tener la extensión de Azure Defender instalada.	La extensión de Azure Defender para Azure Arc proporciona protección contra amenazas para los clústeres de Kubernetes habilitados para Arc. La extensión recopila datos de los nodos del clúster y los envía al back-end de Azure Defender para Kubernetes en la nube para su posterior análisis. Puede encontrar más información en https://docs.microsoft.com/azure/security-center/defender-for-kubernetes-azure-arc.	AuditIfNotExists, Disabled	3.0.0-preview
Se debe habilitar Azure Defender para App Service	Azure Defender para App Service aprovecha la escalabilidad de la nube, y la visibilidad que ofrece Azure como proveedor de servicios en la nube, para supervisar si se producen ataques comunes a aplicaciones web.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores de Azure SQL Database	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para registros de contenedor	Azure Defender para registros de contenedor proporciona análisis de vulnerabilidades de las imágenes extraídas en los últimos 30 días, insertadas en el registro o importadas, y expone los hallazgos detallados por imagen.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para DNS	Azure Defender para DNS proporciona una capa adicional de protección para los recursos en la nube mediante la supervisión continua de todas las consultas de DNS de	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
	los recursos de Azure. Azure Defender alerta sobre las actividades sospechosas en la capa de DNS. Obtenga más información sobre las funcionalidades de Azure Defender para DNS en https://aka.ms/defender-for-dns. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .		
Se debe habilitar Azure Defender para Key Vault	Azure Defender para Key Vault proporciona un nivel de protección adicional de inteligencia de seguridad, ya que detecta intentos inusuales y potencialmente dañinos de obtener acceso a las cuentas de Key Vault o aprovechar sus vulnerabilidades de seguridad.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Kubernetes	Azure Defender para Kubernetes proporciona protección en tiempo real contra amenazas para entornos en contenedores y genera alertas en caso de actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para Resource Manager	Azure Defender para Resource Manager supervisa automáticamente las operaciones de administración de recursos de la organización. Azure Defender detecta amenazas y alerta sobre actividades sospechosas. Obtenga más información sobre las funcionalidades de Azure Defender para Resource Manager en https://aka.ms/defender-for-resource-manager. La habilitación de este plan de Azure Defender conlleva cargos. Obtenga información sobre los detalles de los precios por región en la página de precios de Security Center: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Se debe habilitar Azure Defender para servidores	Azure Defender para SQL proporciona funcionalidad para mostrar y mitigar posibles vulnerabilidades de base de datos, detectar actividades anómalas que podrían indicar	AuditIfNotExists, Disabled	1.0.2

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
SQL Server en las máquinas	amenazas para bases de datos SQL, y detectar y clasificar datos confidenciales.		
Se debe habilitar Azure Defender para SQL en las instancias de Azure SQL Server desprotegidas	Auditoría de los servidores de SQL sin Advanced Data Security	AuditIfNotExists, Disabled	2.0.1
Azure Defender para SQL debe habilitarse en las instancias de SQL Managed Instances desprotegidas.	Permite auditr cada servicio SQL Managed Instance sin Advanced Data Security.	AuditIfNotExists, Disabled	1.0.2
Se debe habilitar Azure Defender para Storage	Azure Defender para Storage detecta intentos inusuales y potencialmente perjudiciales de acceder a las cuentas de almacenamiento o de vulnerarlas.	AuditIfNotExists, Disabled	1.0.3
La extensión "Configuración de invitado" debe estar instalada en las máquinas.	Para garantizar la seguridad de la configuración de invitado, instale la extensión "Configuración de invitado". La configuración de invitado supervisada en la extensión engloba la configuración del sistema operativo, la configuración o presencia de las aplicaciones y la configuración del entorno. Una vez instaladas, las directivas de invitado estarán disponibles como "La protección contra vulnerabilidades de Windows debe estar habilitada.". Obtenga más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1
Los problemas de estado del agente de Log Analytics se deben resolver en sus máquinas	Security Center usa el agente de Log Analytics, que anteriormente se denominaba Microsoft Monitoring Agent (MMA). Para tener la certeza de que las máquinas virtuales tienen la supervisión correcta, es preciso asegurarse de que el agente está instalado en ellas y de que recopila adecuadamente los eventos de seguridad en el área de trabajo configurada.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Linux de Azure Arc	Esta directiva audita las máquinas Linux de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
El agente de Log Analytics debe instalarse en la máquina virtual para la supervisión de Azure Security Center .	Esta directiva audita cualquier máquina virtual Windows o Linux si el agente de Log Analytics no está instalado y Security Center la utiliza para supervisar las amenazas y vulnerabilidades de seguridad	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe instalarse en sus conjuntos de escalado de máquinas virtuales para supervisar Azure Security Center .	Security Center recopila datos de las máquinas virtuales de Azure para supervisar las amenazas y vulnerabilidades de la seguridad.	AuditIfNotExists, Disabled	1.0.0
El agente de Log Analytics debe estar instalado en las máquinas Windows de Azure Arc	Esta directiva audita las máquinas Windows de Azure Arc si el agente de Log Analytics no está instalado.	AuditIfNotExists, Disabled	1.0.0-preview
Control administrado por Microsoft 1683: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1684: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1685: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1686: supervisión	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
del sistema de información			
Control administrado por Microsoft 1687: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1688: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1689: supervisión del sistema de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
El agente de recopilación de datos de tráfico de red debe instalarse en máquinas virtuales Linux .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
El agente de recopilación de datos de tráfico de red debe instalarse en las máquinas virtuales Windows .	Security Center usa Microsoft Dependency Agent para recopilar datos del tráfico de red de sus máquinas virtuales de Azure y así poder habilitar características avanzadas de protección de red, como la visualización del tráfico en el mapa de red, las recomendaciones de refuerzo de la red y las amenazas de red específicas.	AuditIfNotExists, Disabled	1.0.1-preview
Network Watcher debe estar habilitado	Network Watcher es un servicio regional que permite supervisar y diagnosticar problemas en un nivel de escenario de red mediante Azure. La supervisión del nivel de escenario permite diagnosticar problemas en una vista de nivel de red de un extremo a otro. Es preciso que se haya creado un grupo de recursos de Network Watcher en todas las regiones en las que haya una red virtual. Si algún grupo de recursos de Network Watcher no está disponible en una región determinada, se habilita una alerta.	AuditIfNotExists, Disabled	3.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La extensión "Configuración de invitado" de las máquinas virtuales debe implementarse con una identidad administrada asignada por el sistema	La extensión Configuración de invitado requiere una identidad administrada asignada por el sistema. Si las máquinas virtuales de Azure incluidas en el ámbito de esta directiva tienen instalada la extensión "Configuración de invitado" pero no tienen una identidad administrada asignada por el sistema, no cumplirán los requisitos establecidos. Más información en https://aka.ms/gcpol.	AuditIfNotExists, Disabled	1.0.1

Sistema de detección de intrusiones en todo el sistema

Id. : NIST SP 800-53 Rev. 4 SI-4 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1690: supervisión del sistema de información | Sistema de detección de intrusiones en todo el sistema	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Herramientas automatizadas para el análisis en tiempo real

Id. : NIST SP 800-53 Rev. 4 SI-4 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1691: supervisión del sistema de información | Herramientas automatizadas para el análisis en tiempo real	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Tráfico de comunicaciones entrantes y salientes

Id. : NIST SP 800-53 Rev. 4 SI-4 (4)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1692: supervisión del sistema de información | Tráfico de comunicaciones entrantes y salientes	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Alertas generadas por el sistema

Id. : NIST SP 800-53 Rev. 4 SI-4 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1693: supervisión del sistema de información | Alertas generadas por el sistema	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Análisis de anomalías de tráfico de comunicaciones

Id. : NIST SP 800-53 Rev. 4 SI-4 (11)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1694: supervisión del sistema de información | Análisis de anomalías de tráfico de comunicaciones	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Alertas automatizadas

Id. : NIST SP 800-53 Rev. 4 SI-4 (12)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
La opción para enviar notificaciones por correo electrónico para alertas de gravedad alta debe estar habilitada.	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, habilite las notificaciones por correo electrónico de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	1.0.1
La opción para enviar notificaciones por correo electrónico al propietario de la suscripción en relación a alertas de gravedad alta debe estar habilitada.	Para asegurarse de que los propietarios de suscripciones reciban una notificación cuando se produzca una vulneración de seguridad potencial en sus suscripciones, establezca notificaciones por correo electrónico a los propietarios de las suscripciones de alertas de gravedad alta en Security Center.	AuditIfNotExists, Disabled	2.0.0
Las suscripciones deben tener una dirección de correo electrónico de contacto para los problemas de seguridad	Para asegurarse de que las personas pertinentes de la organización reciban una notificación cuando se produzca una vulneración de seguridad potencial en una de las suscripciones, establezca un contacto de seguridad para la recepción de notificaciones por correo electrónico de Security Center.	AuditIfNotExists, Disabled	1.0.1

Detección de intrusiones inalámbricas

Id. : NIST SP 800-53 Rev. 4 SI-4 (14)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1695: supervisión del sistema de información | Detección de intrusiones inalámbricas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Correlación de información de supervisión

Id. : NIST SP 800-53 Rev. 4 SI-4 (16)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1696: supervisión del sistema de información | Correlación de información de supervisión	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Análisis del tráfico o exfiltración de la cobertura

Id. : NIST SP 800-53 Rev. 4 SI-4 (18)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1697: supervisión del sistema de información | Análisis del tráfico o exfiltración de la cobertura	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Individuos que plantean más riesgos

Id. : NIST SP 800-53 Rev. 4 SI-4 (19)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1698: supervisión del sistema de información | Individuos que plantean más riesgos	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Usuarios con privilegios

Id. : NIST SP 800-53 Rev. 4 SI-4 (20)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1699: supervisión del sistema de información | Usuarios con privilegios	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Servicios de red no autorizados

Id. : NIST SP 800-53 Rev. 4 SI-4 (22)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1700: supervisión del sistema de información | Servicios de red no autorizados	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Dispositivos basados en host

Id. : NIST SP 800-53 Rev. 4 SI-4 (23)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1701: supervisión del sistema de información | Dispositivos basados en host	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Indicadores de compromiso

Id. : NIST SP 800-53 Rev. 4 SI-4 (24)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1702: supervisión del sistema de información | Indicadores de compromiso	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Alertas de seguridad, avisos y directivas

Id. : NIST SP 800-53 Rev. 4 SI-5

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1703: alertas, avisos y directivas de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1704: alertas, avisos y directivas de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1705: alertas, avisos y directivas de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1706: alertas, avisos y directivas de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Alertas y advertencias automatizadas

Id. : NIST SP 800-53 Rev. 4 SI-5 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1707: alertas, avisos y directivas de seguridad | Alertas y advertencias automatizadas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Comprobación de la función de seguridad

Id. : NIST SP 800-53 Rev. 4 SI-6

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1708: comprobación de la función de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1709: comprobación de la función de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1710: comprobación de la función de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1711: comprobación de la función de seguridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Integridad de la información, el firmware y el software

Id. : NIST SP 800-53 Rev. 4 SI-7

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1712: integridad de la información, el firmware y el software	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Comprobaciones de integridad

Id. : NIST SP 800-53 Rev. 4 SI-7 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1713: integridad de la información, el firmware y el software | Comprobaciones de integridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Notificaciones automatizadas de infracciones de integridad

Id. : NIST SP 800-53 Rev. 4 SI-7 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1714: integridad de la información, el firmware y el software | Notificaciones automatizadas de infracciones de integridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Respuesta automática a infracciones de integridad

Id. : NIST SP 800-53 Rev. 4 SI-7 (5)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1715: integridad de la información, el firmware y el software | Respuesta automática a infracciones de integridad	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Integración de detección y respuesta

Id. : NIST SP 800-53 Rev. 4 SI-7 (7)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1716: integridad de la información, el firmware y el software | Integración de detección y respuesta	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Código ejecutable de máquina o binario

Id. : NIST SP 800-53 Rev. 4 SI-7 (14)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1717: integridad de la información, el firmware y el software | Código ejecutable de máquina o binario	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1718: integridad de la información, el firmware y el software | Código ejecutable de máquina o binario	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Protección de correo no deseado

Id. : NIST SP 800-53 Rev. 4 SI-8

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1719: protección contra correo no deseado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1720: protección contra correo no deseado	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Administración central

Id. : NIST SP 800-53 Rev. 4 SI-8 (1)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1721: protección contra correo no deseado | Administración central	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Actualizaciones automáticas

Id. : NIST SP 800-53 Rev. 4 SI-8 (2)

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1722: protección contra correo no deseado | Actualizaciones automáticas	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Validación de la entrada de información

Id. : NIST SP 800-53 Rev. 4 SI-10

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1723: validación de la entrada de información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Tratamiento de errores

Id. : NIST SP 800-53 Rev. 4 SI-11

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1724: control de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
Control administrado por Microsoft 1725: control de errores	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Retención y tratamiento de la información

Id. : NIST SP 800-53 Rev. 4 SI-12

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Control administrado por Microsoft 1726: retención y tratamiento de la información	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0

Protección de la memoria

Id. : NIST SP 800-53 Rev. 4 SI-16

Nombre (Azure Portal)	Descripción	Efectos	Versión (GitHub)
Se debe habilitar Azure Defender para servidores	Azure Defender para servidores proporciona protección en tiempo real contra amenazas para las cargas de trabajo del servidor y genera recomendaciones de protección, así como alertas sobre la actividad sospechosa.	AuditIfNotExists, Disabled	1.0.3
Control administrado por Microsoft 1727: protección de la memoria	Microsoft implementa este control de integridad del sistema y de la información	auditoría	1.0.0
La Protección contra vulnerabilidades de seguridad de Windows Defender debe estar habilitada en las máquinas .	La protección contra vulnerabilidades de seguridad de Windows Defender utiliza el agente de configuración de invitado de Azure Policy. La protección contra vulnerabilidades de seguridad tiene cuatro componentes diseñados para bloquear dispositivos en una amplia variedad de vectores de ataque y comportamientos de bloque utilizados habitualmente en ataques de malware, al tiempo que permiten a las empresas equilibrar los requisitos de productividad y riesgo de seguridad (solo Windows).	AuditIfNotExists, Disabled	1.1.1

Pasos siguientes

Artículos adicionales sobre Azure Policy:

- Introducción al Cumplimiento normativo.
- Consulte la estructura de definición de la iniciativa.
- Consulte más ejemplos en Ejemplos de Azure Policy.
- Vea la Descripción de los efectos de directivas.

- Obtenga información sobre cómo corregir recursos no compatibles.

Category	Subcategory	Informative References	AWS Implementation/Enablers/Processes	AWS Services and Responsibility	Customer Responsibility
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8	AWS Certifications, AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch Logs, Customer Responsibility	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer to ISO 27001 standards; Annex A, domain 8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	**CM-8:** AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of system components for their systems. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
	ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8	AWS Certifications, AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch Logs, Customer Responsibility	AWS has established an information security framework and policies and has effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v3.1 and the National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems).	**CM-8:** AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of system components for their systems. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
	ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4	AWS Certifications, Customer Responsibility	AWS Customers designate in which physical region their content will be located. AWS will not move customers' content from the selected regions without notifying the customer, unless required to comply with the law or requests of governmental entities. Boundary protection devices that employ rule sets, access control lists (ACL), and	**AC-4:**AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network Access Control Lists (ACL) for controlling inbound/outbound traffic at the subnet level and Amazon VPC security groups for controlling traffic at the instance level.
	ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6	AWS Certifications, Customer Responsibility		**AC-20:** AWS customers are responsible for establishing terms and conditions with other organizations owning, operating, and/or maintaining external information systems. Consistent with any trust relationships established with these external organizations and in accordance with their access control policy AWS customers are responsible for authorizing individuals
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6	AWS Tagging, Customer Responsibility	AWS customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise,
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3	AWS Certifications, IAM Policies, Customer Responsibility	In alignment with ISO 27001 standard, all AWS employees complete periodic role based training that includes AWS Security training and requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to SOC reports for additional details.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise,
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1**: The organization's role in the supply chain is identified and communicated	• COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05	AWS Certifications, Customer Responsibility	In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers. Refer	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information,
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is	• COBIT 5 APO02.06, APO03.01	AWS Certifications, Customer Responsibility	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with	**PM-8:** AWS customers are responsible for prioritizing critical assets, and developing a critical infrastructure and key resources protection strategy plan.
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6	Customer Responsibility	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that	**PM-11:** AWS customers are responsible for determining information protection needs with regards to the required security controls for the organization and the associated information systems supporting the business processes. In addition, AWS customers are responsible for revising the information protection needs process as needed.
	ID.BE-4: Dependencies and critical functions for delivery of critical services are	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3	AWS Certifications, AWS Best Practices & Reference Architectures, Customer Responsibility	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with	**CP-8, PE-9, PE-11:** Customers are not responsible for these controls as they will be inherited from AWS.
	ID.BE-5: Resilience requirements to support delivery of critical services are established	• COBIT 5 DSS04.02 • ISO/IEC 27001:2013 A.11.1.4, A.17.1.1,	AWS Certifications, AWS Best Practices & Reference Architectures, Customer Responsibility	AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards. Refer to ISO 27001 standard, annex A domain 17 for further details on AWS and business continuity.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information,
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	• COBIT 5 APO01.03, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6	AWS Certifications, AWS Best Practices & Reference Architectures, Customer Responsibility	AWS has established information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for	**All -1 Controls:** AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing an access control policy and supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization.
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3	AWS Certifications, Customer Responsibility	AWS provides security policies and security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Cloud	**PM-1:** AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing an access control policy and supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization.
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7	AWS Certifications, Customer Responsibility	AWS's alignment with ISO 27018 has been validated by an independent third party assessor. ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to Personally Identifiable	**All -1 Controls except PM-1:** AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing a risk assessment policy along with supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization.
	ID.GV-4: Governance and risk management processes address cybersecurity risks	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3,	AWS Certifications, Customer Responsibility	AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to	**PM-9:** AWS customers are responsible for developing a risk management strategy and implementing this strategy across the organization. In addition, AWS customers are responsible for reviewing and updating the risk management strategy in accordance with their organizations policy.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04	AWS Certifications, Customer Responsibility	AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems.	**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the assessment environment, the assessment team, and the assessment roles and responsibilities, 2) Assessing security controls in their system and its environment of operation at an organization-
	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12	AWS Certifications, Customer Responsibility		**PM-15:** AWS customers are responsible for maintaining ongoing contract with security groups and associations to; 1) Facilitate ongoing security education and training for organizational personnel, 2) Maintain currency with recommended security practices, techniques, and technologies, and 3)Share current security-related information including threats,
	ID.RA-3: Threats, both internal and external, are identified and documented	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04	AWS Certifications, Customer Responsibility, AWS Trusted Advisor	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat	**RA-3:** AWS customers are responsible for: 1) Conducting an assessment of risk to include the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of their information system and the information it processes, stores, or transmits, 2) Documenting risk assessment results in the system plan, security
	ID.RA-4: Potential business impacts and likelihoods are identified	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9,	AWS Certifications, Customer Responsibility	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat	**RA-2: AWS customers are responsible for: 1) Categorizing their information and their information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, 2) Documenting the security categorization results (including supporting rationale) in the security plan for the information**
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1	AWS Certifications, Customer Responsibility	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat	**RA-2:** AWS customers are responsible for: 1) Categorizing their information and their information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, 2) Documenting the security categorization results (including supporting rationale) in the security plan for the information system, and 3)
	ID.RA-6: Risk responses are identified and prioritized	• COBIT 5 APO12.05, APO13.02	AWS Certifications, Customer Responsibility	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties	**PM-4:** AWS customers are responsible for; 1) Developing and maintaining a plan of action and milestones program, 2) Documenting the remediation actions taken, and 3) Reporting findings in accordance with OMB FISMA requirements. In
	ID.RM-1: Risk management processes are established, managed, and agreed to by	• COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02	AWS Certifications, Customer Responsibility	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with	**PM-9:** AWS customers are responsible for developing a risk management strategy and implementing this strategy across the organization. In addition, AWS customers are responsible for reviewing and updating the risk management strategy in

	organizational stakeholders			ISO 27018 demonstrates to customers that AWS has a system of controls in place that	accordance with their organizations policy.
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5	AWS Certifications, Customer Responsibility	In alignment with ISO 27001 standard, AWS maintains a Risk Management program to mitigate and manage risk. In addition AWS maintains an AWS ISO 27018 certification. Alignment with ISO 27018 demonstrates to customers that AWS has a system of controls in place that	**PM-9:** AWS customers are responsible for developing a risk management strategy and implementing this strategy across the organization. In addition, AWS customers are responsible for reviewing and updating the risk management strategy in accordance with their organizations policy.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-3**: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14	AWS Certifications, Customer Responsibility	Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard. Refer to ISO 27001 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.	**PM-8:** AWS customers are responsible for prioritizing critical assets, and developing a critical infrastructure and key resources protection strategy plan. **PM-9:** AWS customers are responsible for developing a risk management strategy and implementing this strategy across the organization. In addition, AWS customers are responsible for reviewing and updating the risk management strategy in accordance with their organizations policy. **PM-11:** AWS customers are responsible for determining information protection needs with regards to the required security controls for the organization and the associated information systems supporting the business processes. In addition, AWS customers are responsible for revising the information protection needs process as needed. **SA-14:** AWS customers are responsible for identifying critical information system components by performing analysis on their EC2 instance at a point defined within their SDLC policy/process. The customer can leverage AWS Artifact, which features a comprehensive list of access-controlled documents relevant to compliance and security in the AWS cloud.

Category	Subcategory	Informative References	AWS Implementation/Enablers/Processes	AWS Services and Responsibility	Customer Responsibility
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3,	AWS IAM Policies & Roles/Customer Responsibility	AWS User access privileges are restricted based on business need and job responsibilities. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function.	**AC-2:** AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications
	PR.AC-2: Physical access to assets is managed and protected	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8	AWS Certifications	Physical access to all AWS data centers housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. Access to facilities is only	**PE-2, PE-3, PE-4, PE-5, PE-6, PE-9:** Customers are not responsible for these controls as they will be inherited from AWS. In addition, customers do not have physical access to AWS assets.
	PR.AC-3: Remote access is managed	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6	AWS Certifications, Customer Responsibility, AWS IAM (MFA)	AWS requires multi-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations. Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and	**AC-17:** AWS customers are responsible for establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed to their systems in accordance with their access control policy. AWS customers are responsible for
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• CCS CSC 12, 15 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1	AWS IAM	AWS User access privileges are restricted based on business need and job responsibilities. AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. New user accounts are created to have minimal access. User access to AWS systems (for	**AC-2:** AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3,	AWS VPC, Security Groups, ACL's/Customer Responsibility	In order to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic, AWS has strategically placed a limited number of access points to the cloud. These customer access points are called API	**AC-4:** AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2	AWS Certifications, Customer Responsibility	AWS has implemented formal, documented security awareness and training policy and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. The security awareness and training policy and	**AT-2:** AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization
	PR.AT-2: Privileged users understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3	AWS Certifications, Customer Responsibility	See PR.AT-1	**AT-3:** AWS customers are responsible for providing role-based security training to personnel with assigned security roles and responsibilities: 1) Before authorizing access or performing assigned duties, 2) When required by information system changes, and 3) At a frequency defined by their organization
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2	AWS Certifications, Customer Responsibility	See PR.AT-1	**PS-7:** AWS customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting
	PR.AT-4: Senior executives understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2	AWS Certifications, Customer Responsibility	See PR.AT-1	**AT-3:** AWS customers are responsible for providing role-based security training to personnel with assigned security roles and responsibilities: 1) Before authorizing access or performing assigned duties, 2) When required by information system changes, and 3) At a frequency defined by their organization
	PR.AT-5: Physical and information security personnel understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2	AWS Certifications	See PR.AT-1	**AT-3:** AWS customers are responsible for providing role-based security training to personnel with assigned security roles and responsibilities: 1) Before authorizing access or performing assigned duties, 2) When required by information system changes, and 3) At a frequency defined by their organization
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect	**PR.DS-1:** Data-at-rest is protected	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06	AWS Certifications, AWS Encryption Services (KMS/EBS/S3/EC-2/RDS/REDSHIFT/DYNAMO DB), Customer Responsibility		**SC-28:** AWS customers are responsible for configuring their systems to protect the confidentiality and/or integrity of organization-defined information at rest in accordance with their system and communications protection policy.
	PR.DS-2: Data-in-transit is protected	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1,	AWS Certifications, AWS Encryption Services (KMS/EBS/S3/EC-2/RDS/REDSHIFT/DYNAMO DB), Customer Responsibility	AWS supports SSL/TLS encryption for all of its API Endpoints and the ability to create encrypted VPN tunnels to connect the customer environment to AWS. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL terminations in AWS GovCloud (US)	**SC-8:** AWS customers are responsible for implementing mechanisms to protect the confidentiality and integrity of transmitted information.
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2	AWS Certifications, Customer Responsibility	In order to ensure asset management inventory and maintenance procedures are properly executed, AWS assets are assigned an owner, tracked and monitored with AWS proprietary inventory management tools. AWS asset owner maintenance procedures are carried out by method of utilizing	**CM-8:** AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of system components for their systems. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2)

the Organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-4:** Adequate capacity to ensure availability is maintained	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2	AWS Reference Architectures & Best Practices, Customer Responsibility	AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (for example, weekly). In addition, the AWS capacity planning model supports planning for future	**AU-4:** AWS customers are responsible for allocating audit record storage capacity in accordance with the audit record storage requirements defined in their audit and accountability policy.
	PR.DS-5: Protections against data leaks are implemented	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2	AWS Certifications, AWS Reference Architectures & Best Practices, Customer Responsibility	AWS treats all Customer content and associated assets as Critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored. We are vigilant about our customers' security and have implemented	**AC-4:** AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network Access Control Lists (ACL) for
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8	AWS Certifications, AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch Logs, Customer Responsibility	AWS treats all Customer content and associated assets as Critical information. AWS services are content agnostic, in that they offer the same high level of security to all customers,	**SI-7:** AWS customers are responsible for employing integrity verification tools to monitor and detect unauthorized changes to organization-defined software, firmware, and information
	PR.DS-7: The development and testing environment(s) are separate from the production environment	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4	AWS VPC, Security Groups, ACL's/Customer Responsibility	The customer controls the creation and separation of development and test environments from production.	**CM-2:** AWS customers are responsible for developing, documenting, and maintaining under configuration control a current baseline configuration of their systems.
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3	AWS Certifications, AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch Logs, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the baseline Configuration Management policies, procedures, systems and technologies used by AWS to document and maintain the configuration of its infrastructure.	**CM-2:** AWS customers are responsible for developing, documenting, and maintaining under configuration control a current baseline configuration of their systems. **CM-3:** AWS customers are responsible for implementing a configuration change control process in accordance with their
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the System Development Lifecycle policies and procedures used by AWS. AWS uses the SDLC documented in NIST SP 800-64 rev 2	**SA-3:** AWS customers are responsible for: 1) Managing their systems using an organization-defined System Development Life Cycle (SDLC) that incorporates information security considerations, 2) Defining and documenting information
	PR.IP-3: Configuration change control processes are in place	• COBIT 5 BAI06.01, BAI01.06 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6	AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch & CloudWatch Logs, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the policies and procedures by which AWS Operates, Maintains, Controls, Approves, Deploys, Reports, and Monitors all changes to its environment and infrastructure.	**CM-3:** AWS customers are responsible for implementing a configuration change control process in accordance with their configuration management policy that includes the following elements: 1) Determination of the types of changes to the information system that are configuration-controlled, 2)
	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3	AWS Best Practices & Reference Architectures, AWS S3, EBS Snapshots, AWS Glacier, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which AWS Operates, Maintains, Controls, provides redundancy for and periodically tests backups and recovery of information.	**CP-4:** AWS customers are responsible for testing their contingency plan at an organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. AWS customers are responsible for reviewing the results of contingency plan testing and initiating corrective actions when needed.
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6	AWS Certifications	FedRAMP and ISO 27001 certifications document in detail the manner in which AWS Operates, Maintains, Controls and provides redundancy and emergency responses for its physical infrastructure.	**PE-10, PE-12, PE-13, PE-14. PE-15, PE-18:** Customers are not responsible for these controls as they will be inherited from AWS.
	PR.IP-6: Data is destroyed according to policy	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.4.4.4 • ISA 62443-3-3:2013 SR 4.2	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which AWS Sanitizes media and destroys data. AWS uses products and procedures that conform with NIST SP 800-88.	**MP-6:** Customers are not responsible for these controls as they will be inherited from AWS. Customers must document their Data Security Management and Data Destruction plans in detail for the data they store in
	PR.IP-7: Protection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner and extent to which AWS continually assesses, documents, improves and reports protection processes.	**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate	• ISO/IEC 27001:2013 A.16.1.6	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner and extent to which AWS shares information	**AC-21:** AWS customers are responsible for defining information sharing circumstances where user discretion is
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• COBIT 5 DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which AWS Incident response and recovery plans and business continuity plans are managed for all AWS infrastructure, vendors and personnel.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration
	PR.IP-10: Response and recovery plans are tested	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which AWS response and recovery plans are tested for all AWS infrastructure, vendors and personnel.	**CP-4:** AWS customers are responsible for testing their contingency plan at an organization-defined frequency using organization-defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan.
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2,	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which Cybersecurity is included for all AWS personnel.	**PS-1:** AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing a personnel security policy along with supporting procedures. AWS customers are responsible for reviewing and updating

	PR.IP-12: A vulnerability management plan is developed and implemented	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which risk and vulnerabilities are assessed,	**RA-3: AWS customers are responsible for: 1) Conducting an assessment of risk to include the likelihood and magnitude of**
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7	AWS Certifications, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which remote maintenance policies for the AWS infrastructure are approved, performed, logged and reviewed so as to assure timeliness and use of only approved and	**MA-2, MA-3, MA-5:** Customers are not responsible for these controls as they will be inherited from AWS. Customers have the responsibility to document in detail the
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8	AWS Certifications, AWS IAM, CloudTrail, AWS CloudWatch & CloudWatch Logs, AWS Config, AWS Config Rules, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which all remote maintenance for the AWS infrastructure is approved, performed, logged and reviewed so as to prevent unauthorized access.	**MA-4:** Customers are not responsible for these controls as they will be inherited from AWS. AWS provides a number of services that customers can use
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4	AWS Resource Tagging, AWS Config, AWS Config Rules, AWS Cloud Formation, AWS CloudTrail, AWS CloudWatch & CloudWatch Logs, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which all audit logs and records for the AWS infrastructure are implemented and reviewed.	**AU-1:** AWS customers are responsible for developing, documenting, maintaining, disseminating, and implementing an audit and accountability policy along with supporting procedures. AWS customers are responsible for reviewing and updating the policy and procedures at a frequency defined by their organization.
	PR.PT-2: Removable media is protected and its use restricted according to policy	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3	N/A	FedRAMP and ISO 27001 certifications document in detail the manner in which all removable media assets for the AWS infrastructure are used and protected.	**MP-2, MP-4, MP-5, MP-7:** Customers are not responsible for these controls as they will be inherited from AWS. Customers are not permitted direct access to any physical
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2,	AWS Certifications, AWS IAM, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which the principle of least privilege is implemented to control access to systems and assets for the AWS infrastructure.	**AC-3:** AWS customers are responsible for configuring their systems to enforce logical access based on approved authorizations and in accordance with their access control policy.
	PR.PT-4: Communications and control networks are protected	• CCS CSC 7 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8,	AWS Certifications, AWS VPC, Security Groups, ACL's, VPC Flowlogs, Customer Responsibility	FedRAMP and ISO 27001 certifications document in detail the manner in which both the communications and control networks for the AWS infrastructure are isolated and protected.	**AC-4:** AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network Access Control Lists (ACL) for

Category	Subcategory	Informative References	AWS Implementation/Enablers/Processes	AWS Services and Responsibility	Customer Responsibility
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3	AWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer ResponsibilityE239	Anomalies and events detection are capabilities for which the customer is responsible. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter. AWS utilizes a wide variety of automated monitoring systems designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points of its infrastructure. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom	**AC-4:** AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network Access Control Lists (ACL) for controlling inbound/outbound traffic at the subnet level and
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3	AWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**AC-4:** AWS customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined personnel or roles in accordance with their audit and accountability policy.
	DE.AE-3: Event data are aggregated and correlated from multiple sources and	• ISA 62443-3-3:2013 SR 6.1	AWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**AU-6:** AWS customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined
	DE.AE-4: Impact of events is determined	• COBIT 5 APO12.06	Customer Responsibility		**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration
	DE.AE-5: Incident alert thresholds are established	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10	AWS Best Practices, AWS Reference Architectures, AWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**IR-4:** AWS customers are responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy. In addition, AWS customers are responsible for coordinating incident handling activities with contingency planning
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• CCS CSC 14, 16 • COBIT 5 DSS05.07	AWS Best Practices, AWS Reference Architectures, AWS Config, AWS ConfigRulesAWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility	Policies, procedures and mechanisms to monitor and protect the AWS network environment are in place. AWS security controls are reviewed by independent external auditors during audits for SOC, PCI DSS, ISO 27001 and FedRAMP compliance.	**AC-2:** AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications they install.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity	• ISA 62443-2-1:2009 4.3.3.3.8	AWS Certifications	The AWS Incident response program (detection, investigation and response to incidents) has been developed in alignment	**CA-7:** AWS customers are responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program in accordance with their security assessment and authorization policy that defines: 1) Metrics to be
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1	AWS Certifications, Customer Responsibility	AWS has established controls to address the threat of inappropriate insider access. All certifications and third-party attestations evaluate logical access preventative and detective	**AC-2:** AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications
	DE.CM-4: Malicious code is detected	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2	AWS Best Practices, AWS Reference Architectures, AWS Config, AWS ConfigRulesAWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**SI-3:** AWS customers are responsible for: 1) Implementing malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; 2) Updating malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; 3) Configuring malicious code protection mechanisms to: a) Perform periodic scans of the information system at an organization-defined frequency and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security
	DE.CM-5: Unauthorized mobile code is detected	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1	AWS Mobile Services, Customer Responsibility		**SC-18:** AWS customers are responsible for defining acceptable and unacceptable mobile code, establishing usage restrictions and implementation guidance for acceptable mobile code, and authorizing, monitoring, and controlling the use of mobile code within their systems.
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4	AWS Certifications, Customer Responsibility	AWS has established controls to address the threat of inappropriate access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how access is controlled and monitored.	**CA-7:** AWS customers are responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program in accordance with their security assessment and authorization policy that defines: 1) Metrics to be monitored, 2) Frequencies for monitoring and reporting, and 3) Personnel or roles responsible for conducting and receiving continuous monitoring analysis information. Pursuant to this continuous monitoring program, AWS customers are responsible for: 1) Establishing and configuring monitoring for defined metrics, 2) Monitoring and conducting assessments as organization-defined frequencies, 3) Conducting ongoing security control assessments, 4) Conducting ongoing security status monitoring of their organization-defined metrics, 5) Correlating and analyzing security-related
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	AWS Best Practices, AWS Reference Architectures, AWS Config, AWS ConfigRulesAWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**AU-12:** AWS customers are responsible for configuring their systems to: 1) Provide audit record generation capabilities for the auditable events defined in AU-2a for all system components where audit capabilities are deployed/required based on the audit and accountability policy, 2) Allow organization-defined personnel or roles to select which auditable events are to be audited by specific components, and 3) Generate audit records for the events defined in AU-2d with the content defined in AU-3. **CA-7:** AWS customers are responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program in accordance with their security assessment and authorization policy that defines: 1) Metrics to be monitored, 2) Frequencies for monitoring and reporting, and 3) Personnel or roles responsible for conducting and receiving continuous monitoring analysis information. Pursuant to this continuous monitoring program, AWS customers are responsible for: 1) Establishing and configuring monitoring for defined metrics, 2) Monitoring and conducting assessments as organization-defined frequencies, 3) Conducting ongoing security control assessments, 4) Conducting ongoing security status monitoring of their organization-defined metrics, 5) Correlating and analyzing security-related information generated by assessments and monitoring, 5) Taking appropriate response actions to address the results of the analysis of security-related information, and 6) Reporting the security status of their organization and the information system to the organization-defined personnel or roles at the organization-defined frequency. **CM-3:** AWS customers are responsible for implementing a configuration change control process in accordance with their configuration management policy that includes the following elements: 1) Determination of the types of changes to the information system that are configuration-controlled, 2) Review of all proposed configuration-controlled changes to the information system and approval or disapproval of such changes with explicit consideration for security impact analyses, 3) Documentation of configuration change decisions associated with the information system, 4) Implementation of approved configuration-controlled changes to the information system, 5) Retention of records of configuration-controlled changes to the information system for an organization-defined time period. **CM-8:** AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined
	DE.CM-8: Vulnerability scans are performed	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7	AWS Certifications, Customer Responsibility	AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities.	**RA-5:** AWS customers are responsible for: 1) Scanning for vulnerabilities in their information system and hosted applications at an organization-defined frequency and/or randomly in accordance with their organization-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported; 2) Employing vulnerability scanning tools and techniques that promote interoperability among tools and automated parts
	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1	AWS Certifications, Customer Responsibility	AWS has implemented a formal, documented incident response policy and program (detection, investigation and response to incidents) in alignment with ISO 27001 standards. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS SOC reports provide additional details on controls in place to restrict system access.	**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the assessment environment, the assessment team, and the assessment roles and responsibilities, 2) Assessing security controls in their system and its environment of operation at an
	DE.DP-2: Detection activities comply with all applicable requirements	• ISA 62443-2-1:2009 4.4.3.2	AWS Certifications, Customer Responsibility		**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a

	all applicable requirements	• ISO/IEC 27001:2013 A.18.1.4			security assessment plan that describes the security controls and control enhancements under assessment, assessment
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-3:** Detection processes are tested	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3	AWS Certifications, Customer Responsibility	Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security.	**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the assessment environment, the assessment team, and the assessment roles and responsibilities, 2) Assessing security controls in their system and its environment of operation at an
	DE.DP-4: Event detection information is communicated to appropriate parties	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1	AWS Certifications, Customer Responsibility		**AU-6:** AWS customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined personnel or roles in accordance with their audit and accountability policy. **CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in
	DE.DP-5: Detection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4	AWS Certifications, Customer Responsibility		**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the assessment environment, the assessment team, and the assessment

Category	Subcategory	Informative References	AWS Implementation/Enablers/Processes	AWS Services and Responsibility	Customer Responsibility
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• CCS CSC 18 • COBIT 5 BAI01.10 • ISA 62443-2-1:2009 4.3.4.5.1	AWS Certifications, Customer Responsibility	AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS utilizes a three-phased approach to manage incidents: 1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. Events originate from several sources such as: • Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers. • Trouble tickets entered by an AWS employee. • Calls to the 24x7x365 technical support hotline. If the event meets incident criteria, the relevant on-call support engineer use Event Management Tool system to start an engagement and page relevant program resolvers (for example, Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause. 2. Recovery Phase - The relevant resolvers will perform break fix to address the incident. After addressing troubleshooting, break fix and affected components, the call leader will assign follow-up documentation and follow-up actions and end the call engagement. 3. Reconstitution Phase – The call leader will declare the recovery phase complete after the relevant fix activities have been addressed. The post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and actions, such as design changes. will be captured in a Correction of Errors (COE) document and tracked to completion. To ensure the effectiveness of the AWS Incident Management plan, AWS conducts incident response testing. This testing provides excellent coverage for the discovery of previously unknown defects and failure modes. In addition, it allows the Amazon Security and Service teams to test the systems for potential customer impact and further prepare staff to handle incidents such as detection and analysis, containment, eradication, and recovery, and post-incident activities.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, 5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and 6) Is reviewed and approved by
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4	AWS Certifications, Customer Responsibility		**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and
	RS.CO-2: Events are reported consistent with established criteria	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2	AWS Certifications, Customer Responsibility		**AU-6:** AWS customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined personnel or roles in accordance with their audit and accountability policy.
	RS.CO-3: Information is shared consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2	AWS Certifications, Customer Responsibility		**CA-2:** AWS customers are responsible for conducting security assessments for their systems. Within this context and in accordance with their security assessment and authorization policy, AWS customers are responsible for: 1) Developing a security assessment plan that describes the security controls and control enhancements under assessment, assessment procedures used to determine effectiveness, the
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.5	AWS Certifications, Customer Responsibility		**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• NIST SP 800-53 Rev. 4 PM-15, SI-5	AWS Certifications, Customer Responsibility		**PM-15:** AWS customers are responsible for maintaining ongoing contract with security groups and associations to; 1) Facilitate ongoing security education and training for organizational personnel, 2) Maintain currency with recommended security practices, techniques, and technologies, and 3) Share current security-related information including threats, vulnerabilities, and incidents. **SI-5:** AWS customers are responsible for: 1) Receiving information system security alerts, advisories, and directives from organization-defined external organizations on an ongoing basis, 2) Generating internal security alerts, advisories, and directives as deemed necessary, 3) Disseminating security alerts, advisories, and directives to organization-defined personnel, roles, organizational elements and/or external organizations, and 4) Implementing security directives in accordance with established time frames or notifying the issuing organization of the degree of noncompliance.
Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1	AWS Best Practices, AWS Reference Architectures, AWS Config, AWS ConfigRulesAWS Cloudwatch, CloudWatch Logs, CloudTrail, VPC Flowlogs, Customer Responsibility		**AU-6:** AWS customers are responsible for reviewing and analyzing audit records at an organization-defined frequency for indications of organization-defined inappropriate or unusual activity and reporting these findings to organization-defined personnel or roles in accordance with their audit and accountability policy. **CA-7:** AWS customers are responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program
	RS.AN-2: The impact of the incident is understood	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	AWS Certifications, Customer Responsibility		**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and
	RS.AN-3: Forensics are performed	• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1	AWS Certifications, Customer Responsibility		**AU-7:** AWS customers are responsible for implementing and configuring an audit reduction and report generation capability that: 1) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents and 2) Does not alter the original content or time ordering of audit records.
	RS.AN-4: Incidents are categorized consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4	AWS Certifications, Customer Responsibility		**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5	AWS Certifications, Customer Responsibility		**IR-4:** AWS customers are responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy. In addition, AWS customers are responsible for coordinating incident handling activities with contingency planning activities; incorporating lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises; and implementing the resulting changes accordingly. **CA-7:** AWS customers are responsible for developing a continuous monitoring strategy and implementing a continuous monitoring program in accordance with their security assessment and authorization policy that defines: 1) Metrics to be monitored, 2) Frequencies for monitoring and reporting, and 3) Personnel or roles responsible for conducting and receiving continuous monitoring analysis information.
	RS.MI-2: Incidents are mitigated	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5	AWS Certifications, Customer Responsibility		
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• ISO/IEC 27001:2013 A.12.6.1	AWS Certifications, Customer Responsibility		
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	AWS Certifications, Customer Responsibility	AWS Incident response management includes post mortem and deep root cause analysis. Results are reviewed by relevant senior management and actions, such as design changes, are captured in a Correction of Errors (COE) document and tracked to completion.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, 5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and 6) Is reviewed and approved by organization-defined personnel or roles in accordance with the contingency planning policy.
	RS.IM-2: Response strategies are updated	• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	AWS Certifications, Customer Responsibility	The AWS Incident Response plan is tested regularly and updated as needed to ensure its effectiveness. The Incident Management planning, testing, and test results are reviewed by third party auditors.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, 5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and 6) Is reviewed and approved by organization-defined personnel or roles in accordance with the contingency planning policy. **IR-4:** AWS customers are responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy. In addition, AWS customers are responsible for coordinating incident handling activities with contingency planning activities; incorporating lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises; and implementing the resulting changes accordingly. **IR-8:** AWS customers are responsible for developing an Incident Response Plan (IRP) that: 1) Provides their organization with a roadmap for implementing its incident response capability, 2) Describes the structure and organization of the incident response capability, 3) Provides a high-level approach for how the incident response capability fits into the overall organization, 4) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions, 5) Defines reportable incidents, 6) Provides metrics for measuring the incident response capability within the organization, 7) Defines the resources and management support needed to effectively maintain and mature an incident response capability, and 8) Is reviewed and approved by organization-defined personnel or roles. Customers are responsible for developing and updating their response plans.

Category	Subcategory	Informative References	AWS Implementation/Enablers/Processes	AWS Services and Responsibility	Customer Responsibility
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity	**RC.RP-1:** Recovery plan is executed during or after an event	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04	AWS Certifications, Customer Responsibility	The three categories comprising the "Recover" function-Recovery Planning, Improvements, and Communications- are capabilities for which the customer is responsible. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter.	**CP-2:** AWS customers are responsible for developing a contingency plan for their system that: 1) Identifies essential missions and business functions and associated contingency requirements, 2) Provides recovery objectives, restoration priorities, and metrics, 3) Addresses contingency roles, responsibilities, and assigned individuals with contact information, 4) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, 5) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and 6) Is reviewed and approved by organization-defined personnel or roles in accordance with the contingency planning policy. **CP-10:** AWS customers are responsible for providing for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. **IR-4:** AWS customers are responsible for implementing an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery in accordance with their incident response policy. In addition, AWS customers are responsible for
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	• COBIT 5 BAI05.07 • ISA 62443-2-1 4.4.3.4	AWS Certifications, Customer Responsibility		
	RC.IM-2: Recovery strategies are updated	• COBIT 5 BAI07.08	AWS Certifications, Customer Responsibility		
Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	• COBIT 5 EDM03.02	Customer Responsibility		
	RC.CO-2: Reputation after an event is repaired	• COBIT 5 MEA03.02	Customer Responsibility		
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• NIST SP 800-53 Rev. 4 CP-2, IR-4	AWS Certifications, Customer Responsibility		

TABLE D-3: SUMMARY — ACCESS CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**		x	x	x	x
AC-2	**Account Management**			x	x	x
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				x	x
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				x	x
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*				x	x
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*				x	x
AC-2(5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*					x
AC-2(6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*					
AC-2(7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*					
AC-2(8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*					
AC-2(9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS*					
AC-2(10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*					
AC-2(11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*					x
AC-2(12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*					x
AC-2(13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*					x
AC-3	**Access Enforcement**			x	x	x
AC-3(1)	*ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6.			
AC-3(2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*					
AC-3(3)	*ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*					
AC-3(4)	*ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*					
AC-3(5)	*ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*					
AC-3(6)	*ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*	x	Incorporated into MP-4 and SC-28.			
AC-3(7)	*ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*					
AC-3(8)	*ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*					
AC-3(9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*					
AC-3(10)	*ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*					
AC-4	**Information Flow Enforcement**				x	x
AC-4(1)	*INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*					
AC-4(2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*					
AC-4(3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*					
AC-4(4)	*INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*					
AC-4(5)	*INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*					
AC-4(6)	*INFORMATION FLOW ENFORCEMENT | METADATA*					
AC-4(7)	*INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*					
AC-4(8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*					
AC-4(9)	*INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*					
AC-4(10)	*INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-4(11)	*INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*					
AC-4(12)	*INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*					
AC-4(13)	*INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*					
AC-4(14)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*					
AC-4(15)	*INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*					
AC-4(16)	*INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*	x	Incorporated into AC-4.			
AC-4(17)	*INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*					
AC-4(18)	*INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*					
AC-4(19)	*INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*					
AC-4(20)	*INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*					
AC-4(21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*					
AC-4(22)	*INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*					
AC-5	**Separation of Duties**				x	x
AC-6	**Least Privilege**				x	x
AC-6(1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*				x	x
AC-6(2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*				x	x
AC-6(3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*					x
AC-6(4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*					
AC-6(5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*				x	x
AC-6(6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*					
AC-6(7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*					
AC-6(8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*					
AC-6(9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*				x	x
AC-6(10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*				x	x
AC-7	**Unsuccessful Logon Attempts**			x	x	x
AC-7(1)	*UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*	x	Incorporated into AC-7.			
AC-7(2)	*UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*					
AC-8	**System Use Notification**			x	x	x
AC-9	**Previous Logon (Access) Notification**					
AC-9(1)	*PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*					
AC-9(2)	*PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*					
AC-9(3)	*PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*					
AC-9(4)	*PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*					
AC-10	**Concurrent Session Control**					x
AC-11	**Session Lock**				x	x
AC-11(1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*				x	x
AC-12	**Session Termination**				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-12(1)	*SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*					
AC-13	**Supervision and Review — Access Control**	x	Incorporated into AC-2 and AU-6.			
AC-14	**Permitted Actions without Identification or Authentication**			x	x	x
AC-14(1)	*PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*	x	Incorporated into AC-14.			
AC-15	**Automated Marking**	x	Incorporated into MP-3.			
AC-16	**Security Attributes**					
AC-16(1)	*SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*					
AC-16(2)	*SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*					
AC-16(3)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*					
AC-16(4)	*SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*					
AC-16(5)	*SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*					
AC-16(6)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*					
AC-16(7)	*SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*					
AC-16(8)	*SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*					
AC-16(9)	*SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*					
AC-16(10)	*SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*					
AC-17	**Remote Access**			x	x	x
AC-17(1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*				x	x
AC-17(2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*				x	x
AC-17(3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*				x	x
AC-17(4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*				x	x
AC-17(5)	*REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*	x	Incorporated into SI-4.			
AC-17(6)	*REMOTE ACCESS | PROTECTION OF INFORMATION*					
AC-17(7)	*REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*	x	Incorporated into AC-3(10).			
AC-17(8)	*REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*	x	Incorporated into CM-7.			
AC-17(9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*					
AC-18	**Wireless Access**			x	x	x
AC-18(1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*				x	x
AC-18(2)	*WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*	x	Incorporated into SI-4.			
AC-18(3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*					
AC-18(4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*					x
AC-18(5)	*WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*					x
AC-19	**Access Control for Mobile Devices**			x	x	x
AC-19(1)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
AC-19(2)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
AC-19(3)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*	x	Incorporated into MP-7.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-19(4)	*ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION*					
AC-19(5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*				x	x
AC-20	**Use of External Information Systems**			x	x	x
AC-20(1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*				x	x
AC-20(2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*				x	x
AC-20(3)	*USE OF EXTERNAL INFORMATION SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*					
AC-20(4)	*USE OF EXTERNAL INFORMATION SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES*					
AC-21	**Information Sharing**				x	x
AC-21(1)	*INFORMATION SHARING | AUTOMATED DECISION SUPPORT*					
AC-21(2)	*INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL*					
AC-22	**Publicly Accessible Content**			x	x	x
AC-23	**Data Mining Protection**					
AC-24	**Access Control Decisions**					
AC-24(1)	*ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION*					
AC-24(2)	*ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY*					
AC-25	**Reference Monitor**		x			

TABLE D-4: SUMMARY — AWARENESS AND TRAINING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**		x	x	x	x
AT-2	**Security Awareness Training**		x	x	x	x
AT-2(1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*		x			
AT-2(2)	*SECURITY AWARENESS | INSIDER THREAT*		x		x	x
AT-3	**Role-Based Security Training**		x	x	x	x
AT-3(1)	*ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS*		x			
AT-3(2)	*ROLE-BASED SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*		x			
AT-3(3)	*ROLE-BASED SECURITY TRAINING | PRACTICAL EXERCISES*		x			
AT-3(4)	*ROLE-BASED SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*		x			
AT-4	**Security Training Records**		x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	x	Incorporated into PM-15.			

TABLE D-5: SUMMARY — AUDIT AND ACCOUNTABILITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**		x	x	x	x
AU-2	**Audit Events**			x	x	x
AU-2(1)	*AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*	x	Incorporated into AU-12.			
AU-2(2)	*AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*	x	Incorporated into AU-12.			
AU-2(3)	*AUDIT EVENTS | REVIEWS AND UPDATES*				x	x
AU-2(4)	*AUDIT EVENTS | PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6(9).			
AU-3	**Content of Audit Records**			x	x	x
AU-3(1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*				x	x
AU-3(2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*					x
AU-4	**Audit Storage Capacity**			x	x	x
AU-4(1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*					
AU-5	**Response to Audit Processing Failures**			x	x	x
AU-5(1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*					x
AU-5(2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*					x
AU-5(3)	*RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*					
AU-5(4)	*RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*					
AU-6	**Audit Review, Analysis, and Reporting**		x	x	x	x
AU-6(1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		x		x	x
AU-6(2)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*	x	Incorporated into SI-4.			
AU-6(3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		x		x	x
AU-6(4)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*		x			
AU-6(5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*		x			x
AU-6(6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*		x			x
AU-6(7)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*		x			
AU-6(8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*		x			
AU-6(9)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*		x			
AU-6(10)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*		x			
AU-7	**Audit Reduction and Report Generation**		x		x	x
AU-7(1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		x		x	x
AU-7(2)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*					
AU-8	**Time Stamps**			x	x	x
AU-8(1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*				x	x
AU-8(2)	*TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-9	**Protection of Audit Information**			x	x	x
AU-9(1)	*PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE* MEDIA					
AU-9(2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*					x
AU-9(3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*					x
AU-9(4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*				x	x
AU-9(5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*					
AU-9(6)	*PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS*					
AU-10	**Non-repudiation**		x			x
AU-10(1)	*NON-REPUDIATION | ASSOCIATION OF IDENTITIES*		x			
AU-10(2)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*		x			
AU-10(3)	*NON-REPUDIATION | CHAIN OF CUSTODY*		x			
AU-10(4)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*		x			
AU-10(5)	*NON-REPUDIATION | DIGITAL SIGNATURES*	x	Incorporated into SI-7.			
AU-11	**Audit Record Retention**			x	x	x
AU-11(1)	*AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*		x			
AU-12	**Audit Generation**			x	x	x
AU-12(1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*					x
AU-12(2)	*AUDIT GENERATION | STANDARDIZED FORMATS*					
AU-12(3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*					x
AU-13	**Monitoring for Information Disclosure**		x			
AU-13(1)	*MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*		x			
AU-13(2)	*MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*		x			
AU-14	**Session Audit**		x			
AU-14(1)	*SESSION AUDIT | SYSTEM START-UP*		x			
AU-14(2)	*SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT*		x			
AU-14(3)	*SESSION AUDIT | REMOTE VIEWING / LISTENING*		x			
AU-15	**Alternate Audit Capability**					
AU-16	**Cross-Organizational Auditing**					
AU-16(1)	*CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*					
AU-16(2)	*CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*					

TABLE D-6: SUMMARY — SECURITY ASSESSMENT AND AUTHORIZATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policies and Procedures**		x	x	x	x
CA-2	**Security Assessments**		x	x	x	x
CA-2(1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		x		x	x
CA-2(2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*		x			x
CA-2(3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*		x			
CA-3	**System Interconnections**		x	x	x	x
CA-3(1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*					
CA-3(5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*				x	x
CA-4	**Security Certification**	x	Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**		x	x	x	x
CA-5(1)	*PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			
CA-6	**Security Authorization**		x	x	x	x
CA-7	**Continuous Monitoring**		x	x	x	x
CA-7(1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		x		x	x
CA-7(2)	*CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*	x	Incorporated into CA-2.			
CA-7(3)	*CONTINUOUS MONITORING | TREND ANALYSES*		x			
CA-8	**Penetration Testing**		x			x
CA-8(1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*		x			
CA-8(2)	*PENETRATION TESTING | RED TEAM EXERCISES*		x			
CA-9	**Internal System Connections**		x	x	x	x
CA-9(1)	*INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*		x			

TABLE D-7: SUMMARY — CONFIGURATION MANAGEMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**		x	x	x	x
CM-2	**Baseline Configuration**		x	x	x	x
CM-2(1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		x		x	x
CM-2(2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			x
CM-2(3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		x		x	x
CM-2(4)	*BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2(5)	*BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2(6)	*BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*		x			
CM-2(7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		x		x	x
CM-3	**Configuration Change Control**		x		x	x
CM-3(1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*		x			x
CM-3(2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		x		x	x
CM-3(3)	*CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*					
CM-3(4)	*CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*					
CM-3(5)	*CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*					
CM-3(6)	*CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*					
CM-4	**Security Impact Analysis**		x	x	x	x
CM-4(1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*		x			x
CM-4(2)	*SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*		x			
CM-5	**Access Restrictions for Change**				x	x
CM-5(1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*					x
CM-5(2)	*ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*					x
CM-5(3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*					x
CM-5(4)	*ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*					
CM-5(5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*					
CM-5(6)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*					
CM-5(7)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS*	x	Incorporated into SI-7.			
CM-6	**Configuration Settings**			x	x	x
CM-6(1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*					x
CM-6(2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*					x
CM-6(3)	*CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*	x	Incorporated into SI-7.			
CM-6(4)	*CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*	x	Incorporated into CM-4.			
CM-7	**Least Functionality**			x	x	x
CM-7(1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*				x	x
CM-7(2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-7(3)	*LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*					
CM-7(4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*				x	
CM-7(5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*					x
CM-8	**Information System Component Inventory**		x	x	x	x
CM-8(1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		x		x	x
CM-8(2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*		x			x
CM-8(3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		x		x	x
CM-8(4)	*INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*		x			x
CM-8(5)	*INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*		x		x	x
CM-8(6)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*		x			
CM-8(7)	*INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*		x			
CM-8(8)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*		x			
CM-8(9)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*		x			
CM-9	**Configuration Management Plan**				x	x
CM-9(1)	*CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*					
CM-10	**Software Usage Restrictions**			x	x	x
CM-10(1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*					
CM-11	**User-Installed Software**			x	x	x
CM-11(1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*					
CM-11(2)	*USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*					

TABLE D-8: SUMMARY — CONTINGENCY PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(6)	*CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*					
CP-2(7)	*CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*					
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-3(2)	*CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		x			
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-4(3)	*CONTINGENCY PLAN TESTING | AUTOMATED TESTING*		x			
CP-4(4)	*CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*		x			
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-7(6)	*ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*					
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-8(5)	*TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*					
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					x
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					x
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	x	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					x
CP-9(6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*					
CP-9(7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*					
CP-10	**Information System Recovery and Reconstitution**			x	x	x
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	x	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				x	x
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	x	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					x
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	x	Incorporated into SI-13.			
CP-10(6)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*					
CP-11	**Alternate Communications Protocols**					
CP-12	**Safe Mode**		x			
CP-13	**Alternative Security Mechanisms**					

TABLE D-9: SUMMARY — IDENTIFICATION AND AUTHENTICATION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-1	**Identification and Authentication Policy and Procedures**		x	x	x	x
IA-2	**Identification and Authentication (Organizational Users)**			x	x	x
IA-2(1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*			x	x	x
IA-2(2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*				x	x
IA-2(3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*				x	x
IA-2(4)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*					x
IA-2(5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*					
IA-2(6)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2(7)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2(8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*				x	x
IA-2(9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*					x
IA-2(10)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON*					
IA-2(11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*				x	x
IA-2(12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*			x	x	x
IA-2(13)	*IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*					
IA-3	**Device Identification and Authentication**				x	x
IA-3(1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*					
IA-3(2)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*	x	Incorporated into IA-3(1).			
IA-3(3)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*					
IA-3(4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*					
IA-4	**Identifier Management**			x	x	x
IA-4(1)	*IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*					
IA-4(2)	*IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*					
IA-4(3)	*IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*					
IA-4(4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*					
IA-4(5)	*IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*					
IA-4(6)	*IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*					
IA-4(7)	*IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*					
IA-5	**Authenticator Management**			x	x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-5(1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*			x	x	x
IA-5(2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*				x	x
IA-5(3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*				x	x
IA-5(4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*					
IA-5(5)	*AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*					
IA-5(6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*					
IA-5(7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*					
IA-5(8)	*AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*					
IA-5(9)	*AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*					
IA-5(10)	*AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*					
IA-5(11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*			x	x	x
IA-5(12)	*AUTHENTICATOR MANAGEMENT | BIOMETRIC-BASED AUTHENTICATION*					
IA-5(13)	*AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*					
IA-5(14)	*AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*					
IA-5(15)	*AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*					
IA-6	**Authenticator Feedback**			x	x	x
IA-7	**Cryptographic Module Authentication**			x	x	x
IA-8	**Identification and Authentication (Non-Organizational Users)**			x	x	x
IA-8(1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*			x	x	x
IA-8(2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*			x	x	x
IA-8(3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*			x	x	x
IA-8(4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*			x	x	x
IA-8(5)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS*					
IA-9	**Service Identification and Authentication**					
IA-9(1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*					
IA-9(2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*					
IA-10	**Adaptive Identification and Authentication**					
IA-11	**Re-authentication**					

TABLE D-10: SUMMARY — INCIDENT RESPONSE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**		x	x	x	x
IR-2	**Incident Response Training**		x	x	x	x
IR-2(1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*		x			x
IR-2(2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		x			x
IR-3	**Incident Response Testing**		x		x	x
IR-3(1)	*INCIDENT RESPONSE TESTING | AUTOMATED TESTING*		x			
IR-3(2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		x		x	x
IR-4	**Incident Handling**			x	x	x
IR-4(1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*				x	x
IR-4(2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*					
IR-4(3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*					
IR-4(4)	*INCIDENT HANDLING | INFORMATION CORRELATION*					x
IR-4(5)	*INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*					
IR-4(6)	*INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*					
IR-4(7)	*INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*					
IR-4(8)	*INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*					
IR-4(9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*					
IR-4(10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*					
IR-5	**Incident Monitoring**		x	x	x	x
IR-5(1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*		x			x
IR-6	**Incident Reporting**			x	x	x
IR-6(1)	*INCIDENT REPORTING | AUTOMATED REPORTING*				x	x
IR-6(2)	*INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*					
IR-6(3)	*INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*					
IR-7	**Incident Response Assistance**			x	x	x
IR-7(1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*				x	x
IR-7(2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*					
IR-8	**Incident Response Plan**			x	x	x
IR-9	**Information Spillage Response**					
IR-9(1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*					
IR-9(2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*					
IR-9(3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*					
IR-9(4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*					
IR-10	**Integrated Information Security Analysis Team**					

TABLE D-11: SUMMARY — MAINTENANCE CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MA-1	**System Maintenance Policy and Procedures**		x	x	x	x
MA-2	**Controlled Maintenance**			x	x	x
MA-2(1)	*CONTROLLED MAINTENANCE | RECORD CONTENT*	x	Incorporated into MA-2.			
MA-2(2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*					x
MA-3	**Maintenance Tools**				x	x
MA-3(1)	*MAINTENANCE TOOLS | INSPECT TOOLS*				x	x
MA-3(2)	*MAINTENANCE TOOLS | INSPECT MEDIA*				x	x
MA-3(3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*					x
MA-3(4)	*MAINTENANCE TOOLS | RESTRICTED TOOL USE*					
MA-4	**Nonlocal Maintenance**			x	x	x
MA-4(1)	*NONLOCAL MAINTENANCE | AUDITING AND REVIEW*					
MA-4(2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*				x	x
MA-4(3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*					x
MA-4(4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*					
MA-4(5)	*NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*					
MA-4(6)	*NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*					
MA-4(7)	*NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*					
MA-5	**Maintenance Personnel**			x	x	x
MA-5(1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*					x
MA-5(2)	*MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*					
MA-5(3)	*MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*					
MA-5(4)	*MAINTENANCE PERSONNEL | FOREIGN NATIONALS*					
MA-5(5)	*MAINTENANCE PERSONNEL | NON-SYSTEM-RELATED MAINTENANCE*					
MA-6	**Timely Maintenance**				x	x
MA-6(1)	*TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*					
MA-6(2)	*TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*					
MA-6(3)	*TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*					

TABLE D-12: SUMMARY — MEDIA PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2(1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4(2).			
MP-2(2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4(1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-4(2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5(1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5(2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5(3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6(1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6(2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6(3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6(4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6(7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6(8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7(2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8(1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8(2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8(3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8(4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

TABLE D-13: SUMMARY — PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		x	x	x	x
PE-2	**Physical Access Authorizations**			x	x	x
PE-2(1)	*PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*					
PE-2(2)	*PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*					
PE-2(3)	*PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*					
PE-3	**Physical Access Control**			x	x	x
PE-3(1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					x
PE-3(2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*					
PE-3(3)	*PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*					
PE-3(4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*					
PE-3(5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*					
PE-3(6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*					
PE-4	**Access Control for Transmission Medium**				x	x
PE-5	**Access Control for Output Devices**				x	x
PE-5(1)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*					
PE-5(2)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*					
PE-5(3)	*ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*					
PE-6	**Monitoring Physical Access**		x	x	x	x
PE-6(1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		x		x	x
PE-6(2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		x			
PE-6(3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		x			
PE-6(4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		x			x
PE-7	**Visitor Control**	x	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		x	x	x	x
PE-8(1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					x
PE-8(2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	x	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				x	x
PE-9(1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*					
PE-9(2)	*POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*					
PE-10	**Emergency Shutoff**				x	x
PE-10(1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	x	Incorporated into PE-10.			
PE-11	**Emergency Power**				x	x
PE-11(1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					x
PE-11(2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-12	**Emergency Lighting**			x	x	x
PE-12(1)	*EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					
PE-13	**Fire Protection**			x	x	x
PE-13(1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					x
PE-13(2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					x
PE-13(3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				x	x
PE-13(4)	*FIRE PROTECTION | INSPECTIONS*					
PE-14	**Temperature and Humidity Controls**			x	x	x
PE-14(1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*					
PE-14(2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*					
PE-15	**Water Damage Protection**			x	x	x
PE-15(1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					x
PE-16	**Delivery and Removal**			x	x	x
PE-17	**Alternate Work Site**				x	x
PE-18	**Location of Information System Components**					x
PE-18(1)	*LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*					
PE-19	**Information Leakage**					
PE-19(1)	*INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*					
PE-20	**Asset Monitoring and Tracking**					

TABLE D-14: SUMMARY — PLANNING CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		x	x	x	x
PL-2	**System Security Plan**		x	x	x	x
PL-2(1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	x	Incorporated into PL-7.			
PL-2(2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	x	Incorporated into PL-8.			
PL-2(3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		x		x	x
PL-3	**System Security Plan Update**	x	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		x	x	x	x
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		x		x	x
PL-5	**Privacy Impact Assessment**	x	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	x	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Information Security Architecture**		x		x	x
PL-8(1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*		x			
PL-8(2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*		x			
PL-9	**Central Management**		x			

TABLE D-15: SUMMARY — PERSONNEL SECURITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**		x	x	x	x
PS-2	**Position Risk Designation**			x	x	x
PS-3	**Personnel Screening**			x	x	x
PS-3(1)	*PERSONNEL SCREENING | CLASSIFIED INFORMATION*					
PS-3(2)	*PERSONNEL SCREENING | FORMAL INDOCTRINATION*					
PS-3(3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*					
PS-4	**Personnel Termination**			x	x	x
PS-4(1)	*PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*					
PS-4(2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*					x
PS-5	**Personnel Transfer**			x	x	x
PS-6	**Access Agreements**		x	x	x	x
PS-6(1)	*ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*	x	Incorporated into PS-3.			
PS-6(2)	*ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*		x			
PS-6(3)	*ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*		x			
PS-7	**Third-Party Personnel Security**		x	x	x	x
PS-8	**Personnel Sanctions**			x	x	x

TABLE D-16: SUMMARY — RISK ASSESSMENT CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**		x	x	x	x
RA-2	**Security Categorization**			x	x	x
RA-3	**Risk Assessment**		x	x	x	x
RA-4	**Risk Assessment Update**	x	Incorporated into RA-3.			
RA-5	**Vulnerability Scanning**		x	x	x	x
RA-5(1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		x		x	x
RA-5(2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		x		x	x
RA-5(3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*		x			
RA-5(4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*		x			x
RA-5(5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		x		x	x
RA-5(6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*		x			
RA-5(7)	*VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*	x	Incorporated into CM-8.			
RA-5(8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*		x			
RA-5(9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	x	Incorporated into CA-8.			
RA-5(10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*		x			
RA-6	**Technical Surveillance Countermeasures Survey**		x			

TABLE D-17: SUMMARY — SYSTEM AND SERVICES ACQUISITION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**		x	x	x	x
SA-2	**Allocation of Resources**		x	x	x	x
SA-3	**System Development Life Cycle**		x	x	x	x
SA-4	**Acquisition Process**		x	x	x	x
SA-4(1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		x		x	x
SA-4(2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		x		x	x
SA-4(3)	*ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*		x			
SA-4(4)	*ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*	x	Incorporated into CM-8(9).			
SA-4(5)	*ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*		x			
SA-4(6)	*ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*		x			
SA-4(7)	*ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*		x			
SA-4(8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*		x			
SA-4(9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		x		x	x
SA-4(10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*		x	x	x	x
SA-5	**Information System Documentation**		x	x	x	x
SA-5(1)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	x	Incorporated into SA-4(1).			
SA-5(2)	*INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*	x	Incorporated into SA-4(2).			
SA-5(3)	*INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*	x	Incorporated into SA-4(2).			
SA-5(4)	*INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*	x	Incorporated into SA-4(2).			
SA-5(5)	*INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*	x	Incorporated into SA-4(2).			
SA-6	**Software Usage Restrictions**	x	Incorporated into CM-10 and SI-7.			
SA-7	**User-Installed Software**	x	Incorporated into CM-11 and SI-7.			
SA-8	**Security Engineering Principles**		x		x	x
SA-9	**External Information System Services**		x	x	x	x
SA-9(1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*		x			
SA-9(2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		x		x	x
SA-9(3)	*EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*		x			
SA-9(4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*		x			
SA-9(5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*		x			
SA-10	**Developer Configuration Management**		x		x	x
SA-10(1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*		x			
SA-10(2)	*DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-10(3)	*DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*		x			
SA-10(4)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*		x			
SA-10(5)	*DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*		x			
SA-10(6)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*		x			
SA-11	**Developer Security Testing and Evaluation**		x		x	x
SA-11(1)	*DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*		x			
SA-11(2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*		x			
SA-11(3)	*DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*		x			
SA-11(4)	*DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*		x			
SA-11(5)	*DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING*		x			
SA-11(6)	*DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*		x			
SA-11(7)	*DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*		x			
SA-11(8)	*DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*		x			
SA-12	**Supply Chain Protection**		x			x
SA-12(1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*		x			
SA-12(2)	*SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*		x			
SA-12(3)	*SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*	x	Incorporated into SA-12(1).			
SA-12(4)	*SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*	x	Incorporated into SA-12(13).			
SA-12(5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*		x			
SA-12(6)	*SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*	x	Incorporated into SA-12(1).			
SA-12(7)	*SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*		x			
SA-12(8)	*SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*		x			
SA-12(9)	*SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*		x			
SA-12(10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*		x			
SA-12(11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*		x			
SA-12(12)	*SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*		x			
SA-12(13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*		x			
SA-12(14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*		x			
SA-12(15)	*SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*		x			
SA-13	**Trustworthiness**		x			
SA-14	**Criticality Analysis**		x			
SA-14(1)	*CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*	x	Incorporated into SA-20.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**		x			x
SA-15(1)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*		x			
SA-15(2)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*		x			
SA-15(3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*		x			
SA-15(4)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*		x			
SA-15(5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*		x			
SA-15(6)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*		x			
SA-15(7)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*		x			
SA-15(8)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*		x			
SA-15(9)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*		x			
SA-15(10)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*		x			
SA-15(11)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*		x			
SA-16	**Developer-Provided Training**		x			x
SA-17	**Developer Security Architecture and Design**		x			x
SA-17(1)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*		x			
SA-17(2)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*		x			
SA-17(3)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*		x			
SA-17(4)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*		x			
SA-17(5)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*		x			
SA-17(6)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*		x			
SA-17(7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*		x			
SA-18	**Tamper Resistance and Detection**		x			
SA-18(1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*		x			
SA-18(2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*		x			
SA-19	**Component Authenticity**		x			
SA-19(1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*		x			
SA-19(2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*		x			
SA-19(3)	*COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*		x			
SA-19(4)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*		x			
SA-20	**Customized Development of Critical Components**		x			
SA-21	**Developer Screening**		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-21(1)	*DEVELOPER SCREENING | VALIDATION OF SCREENING*		x			
SA-22	**Unsupported System Components**		x			
SA-22(1)	*UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*		x			

TABLE D-18: SUMMARY — SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**		x	x	x	x
SC-2	**Application Partitioning**		x		x	x
SC-2(1)	*APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*		x			
SC-3	**Security Function Isolation**		x			x
SC-3(1)	*SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*		x			
SC-3(2)	*SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*		x			
SC-3(3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*		x			
SC-3(4)	*SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*		x			
SC-3(5)	*SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*		x			
SC-4	**Information in Shared Resources**				x	x
SC-4(1)	*INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*	x	Incorporated into SC-4.			
SC-4(2)	*INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*					
SC-5	**Denial of Service Protection**			x	x	x
SC-5(1)	*DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*					
SC-5(2)	*DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*					
SC-5(3)	*DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*					
SC-6	**Resource Availability**		x			
SC-7	**Boundary Protection**			x	x	x
SC-7(1)	*BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*	x	Incorporated into SC-7.			
SC-7(2)	*BOUNDARY PROTECTION | PUBLIC ACCESS*	x	Incorporated into SC-7.			
SC-7(3)	*BOUNDARY PROTECTION | ACCESS POINTS*				x	x
SC-7(4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*				x	x
SC-7(5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*				x	x
SC-7(6)	*BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*	x	Incorporated into SC-7(18).			
SC-7(7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*				x	x
SC-7(8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*					x
SC-7(9)	*BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*					
SC-7(10)	*BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*					
SC-7(11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*					
SC-7(12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*					
SC-7(13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*					
SC-7(14)	*BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*					
SC-7(15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*					
SC-7(16)	*BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-7(17)	*BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*					
SC-7(18)	*BOUNDARY PROTECTION | FAIL SECURE*		x			x
SC-7(19)	*BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*					
SC-7(20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*					
SC-7(21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*		x			x
SC-7(22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*		x			
SC-7(23)	*BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*					
SC-8	**Transmission Confidentiality and Integrity**				x	x
SC-8(1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*				x	x
SC-8(2)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*					
SC-8(3)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*					
SC-8(4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*					
SC-9	**Transmission Confidentiality**	x	Incorporated into SC-8.			
SC-10	**Network Disconnect**				x	x
SC-11	**Trusted Path**		x			
SC-11(1)	*TRUSTED PATH | LOGICAL ISOLATION*		x			
SC-12	**Cryptographic Key Establishment and Management**			x	x	x
SC-12(1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*					x
SC-12(2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*					
SC-12(3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*					
SC-12(4)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*	x	Incorporated into SC-12.			
SC-12(5)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*	x	Incorporated into SC-12.			
SC-13	**Cryptographic Protection**			x	x	x
SC-13(1)	*CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*	x	Incorporated into SC-13.			
SC-13(2)	*CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*	x	Incorporated into SC-13.			
SC-13(3)	*CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*	x	Incorporated into SC-13.			
SC-13(4)	*CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*	**x**	Incorporated into SC-13.			
SC-14	**Public Access Protections**	**x**	Capability provided by AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.			
SC-15	**Collaborative Computing Devices**			x	x	x
SC-15(1)	*COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*					
SC-15(2)	*COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*	x	Incorporated into SC-7.			
SC-15(3)	*COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-15(4)	*COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*					
SC-16	**Transmission of Security Attributes**					
SC-16(1)	*TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*					
SC-17	**Public Key Infrastructure Certificates**				x	x
SC-18	**Mobile Code**				x	x
SC-18(1)	*MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*					
SC-18(2)	*MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*					
SC-18(3)	*MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*					
SC-18(4)	*MOBILE CODE | PREVENT AUTOMATIC EXECUTION*					
SC-18(5)	*MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*					
SC-19	**Voice Over Internet Protocol**				x	x
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**			x	x	x
SC-20(1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*	x	Incorporated into SC-20.			
SC-20(2)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*					
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**			x	x	x
SC-21(1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*	x	Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**			x	x	x
SC-23	**Session Authenticity**				x	x
SC-23(1)	*SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*					
SC-23(2)	*SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*	x	Incorporated into AC-12(1).			
SC-23(3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*					
SC-23(4)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	x	Incorporated into SC-23(3).			
SC-23(5)	*SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*					
SC-24	**Fail in Known State**		x			x
SC-25	**Thin Nodes**					
SC-26	**Honeypots**					
SC-26(1)	*HONEYPOTS | DETECTION OF MALICIOUS CODE*	x	Incorporated into SC-35.			
SC-27	**Platform-Independent Applications**					
SC-28	**Protection of Information at Rest**				x	x
SC-28(1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*					
SC-28(2)	*PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*					
SC-29	**Heterogeneity**		x			
SC-29(1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*		x			
SC-30	**Concealment and Misdirection**		x			
SC-30(1)	*CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*	x	Incorporated into SC-29(1).			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-30(2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*		x			
SC-30(3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*		x			
SC-30(4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*		x			
SC-30(5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*		x			
SC-31	**Covert Channel Analysis**		x			
SC-31(1)	*COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*		x			
SC-31(2)	*COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*		x			
SC-31(3)	*COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*		x			
SC-32	**Information System Partitioning**		x			
SC-33	**Transmission Preparation Integrity**	x	Incorporated into SC-8.			
SC-34	**Non-Modifiable Executable Programs**		x			
SC-34(1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*		x			
SC-34(2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*		x			
SC-34(3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*		x			
SC-35	**Honeyclients**					
SC-36	**Distributed Processing and Storage**		x			
SC-36(1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*		x			
SC-37	**Out-of-Band Channels**		x			
SC-37(1)	*OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*		x			
SC-38	**Operations Security**		x			
SC-39	**Process Isolation**		x	x	x	x
SC-39(1)	*PROCESS ISOLATION | HARDWARE SEPARATION*		x			
SC-39(2)	*PROCESS ISOLATION | THREAD ISOLATION*		x			
SC-40	**Wireless Link Protection**					
SC-40(1)	*WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*					
SC-40(2)	*WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*					
SC-40(3)	*WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*					
SC-40(4)	*WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*					
SC-41	**Port and I/O Device Access**					
SC-42	**Sensor Capability and Data**					
SC-42(1)	*SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*					
SC-42(2)	*SENSOR CAPABILITY AND DATA | AUTHORIZED USE*					
SC-42(3)	*SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*					
SC-43	**Usage Restrictions**					
SC-44	**Detonation Chambers**					

TABLE D-19: SUMMARY — SYSTEM AND INFORMATION INTEGRITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**		x	x	x	x
SI-2	**Flaw Remediation**			x	x	x
SI-2(1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*					x
SI-2(2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*				x	x
SI-2(3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*					
SI-2(4)	*FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*	x	Incorporated into SI-2.			
SI-2(5)	*FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*					
SI-2(6)	*FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*					
SI-3	**Malicious Code Protection**			x	x	x
SI-3(1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-3(2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*				x	x
SI-3(3)	*MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*	x	Incorporated into AC-6(10).			
SI-3(4)	*MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*					
SI-3(5)	*MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
SI-3(6)	*MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*					
SI-3(7)	*MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*					
SI-3(8)	*MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*					
SI-3(9)	*MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*					
SI-3(10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*					
SI-4	**Information System Monitoring**		x	x	x	x
SI-4(1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*		x			
SI-4(2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		x		x	x
SI-4(3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*		x			
SI-4(4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		x		x	x
SI-4(5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		x		x	x
SI-4(6)	*INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*	x	Incorporated into AC-6(10).			
SI-4(7)	*INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*		x			
SI-4(8)	*INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*	x	Incorporated into SI-4.			
SI-4(9)	*INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*		x			
SI-4(10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*		x			
SI-4(11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*		x			
SI-4(12)	*INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*		x			
SI-4(13)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*		x			
SI-4(14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-4(15)	*INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*		x			
SI-4(16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*		x			
SI-4(17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*		x			
SI-4(18)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*		x			
SI-4(19)	*INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*		x			
SI-4(20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*		x			
SI-4(21)	*INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*		x			
SI-4(22)	*INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*		x			
SI-4(23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*		x			
SI-4(24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*		x			
SI-5	**Security Alerts, Advisories, and Directives**		x	x	x	x
SI-5(1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*		x			x
SI-6	**Security Function Verification**		x			x
SI-6(1)	*SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*	x	Incorporated into SI-6.			
SI-6(2)	*SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*					
SI-6(3)	*SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*					
SI-7	**Software, Firmware, and Information Integrity**		x		x	x
SI-7(1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		x		x	x
SI-7(2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*		x			x
SI-7(3)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS*		x			
SI-7(4)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*	x	Incorporated into SA-12.			
SI-7(5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*		x			x
SI-7(6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*		x			
SI-7(7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		x		x	x
SI-7(8)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*		x			
SI-7(9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*		x			
SI-7(10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*		x			
SI-7(11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*		x			
SI-7(12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-7(13)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*		x			
SI-7(14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*		x			x
SI-7(15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*		x			
SI-7(16)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*		x			
SI-8	**Spam Protection**				x	x
SI-8(1)	*SPAM PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-8(2)	*SPAM PROTECTION | AUTOMATIC UPDATES*				x	x
SI-8(3)	*SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*					
SI-9	**Information Input Restrictions**	x	Incorporated into AC-2, AC-3, AC-5, AC-6.			
SI-10	**Information Input Validation**		x		x	x
SI-10(1)	*INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*		x			
SI-10(2)	*INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*		x			
SI-10(3)	*INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*		x			
SI-10(4)	*INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*		x			
SI-10(5)	*INFORMATION INPUT VALIDATION | REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*		x			
SI-11	**Error Handling**				x	x
SI-12	**Information Handling and Retention**			x	x	x
SI-13	**Predictable Failure Prevention**		x			
SI-13(1)	*PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*		x			
SI-13(2)	*PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	x	Incorporated into SI-7(16).			
SI-13(3)	*PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*		x			
SI-13(4)	*PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*		x			
SI-13(5)	*PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*		x			
SI-14	**Non-Persistence**		x			
SI-14(1)	*NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*		x			
SI-15	**Information Output Filtering**		x			
SI-16	**Memory Protection**		x		x	x
SI-17	**Fail-Safe Procedures**		x			

ADJUSTMENTS TO SECURITY CONTROL BASELINES

ALLOCATION OF SECURITY CONTROLS AND ASSIGNMENT OF PRIORITY SEQUENCING CODES

With each revision to SP 800-53, minor adjustments may occur with the security control baselines including, for example, allocating additional controls and/or control enhancements, eliminating selected controls/enhancements, and changing sequencing priority codes (P-codes). These changes reflect: (i) the ongoing receipt and analysis of threat information; (ii) the periodic reexamination of the initial assumptions that generated the security control baselines; (iii) the desire for common security control baseline starting points for national security and non-national security systems to achieve community-wide convergence (relying subsequently on specific overlays to describe any adjustments from the common starting points); and (iv) the periodic reassessment of priority codes to appropriately balance the workload of security control implementation. Over time, as the security control catalog expands to address the continuing challenges from a dynamic and growing threat space that is increasingly sophisticated, organizations will come to rely to a much greater degree on overlays to provide the needed specialization for their security plans.