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 artículo
DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL , APLICANDO ISO 27002 y CSF de NITS
Línea de Investigación:
Seguridad de la Información e Informática
Campo amplio de conocimiento:
Tecnologías de la información y Comunicación (TIC)
Autor:
Daniel Alejandro Hernández Mera
Tutor:
Msc. Ing. Pablo Recalde V

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 Y CSF DE NITS.

Elaborado por: Daniel Alejandro Hernández Mera, con C.I: 1002851754 estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, 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 2023

Firma

ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Daniel Alejandro Hernández Mera con C.I: 1002851754, autor del proyecto de titulación denominado: Diseño de un Esquema de Seguridad Informática para el Área de Sistematización de la Universidad Israel, Aplicando ISO 27002 Y CSF De NITS. Previo a la obtención del título de Magister en Seguridad Informática.

1. 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.
2. 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 autor 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.
3. 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 2023

Firma

ORCID: 0009-0002-2182-7851

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

En la actualidad las entidades buscan crecer y alcanzar objetivos mediante la incorporación de la tecnología de vanguardia en sus procesos, lo cual permita ser competentes y productivos, pero esto conlleva diseñar esquemas de seguridad informática para garantizar los principios básicos como la integridad, confidencialidad y disponibilidad de la información.

Contextualización del tema

Según Zapata & Ríos (2019) afirman que: La norma ISO27002 es fundamental debido a brinda un conjunto de buenas prácticas para la conservación de un Sistemas de Gestión de la Seguridad de la Información (SGSI), por lo cual se vuelve esencial su implementación en toda entidad que manejen sistemas informáticos, para así promover un ambiente seguro y estable, mitigando las vulnerabilidades y riesgos a los que se encuentran expuestas las Organizaciones.

El marco de Cybersecurity Framework del National Institute of Standards and Technology (CSF de NIST) contempla las mejores prácticas de ciberseguridad por lo cual es considerado una herramienta de gestión de riesgos de ciberseguridad, ya que debido a su flexibilidad pude adaptarse a cualquier tipo de organización independientemente de su tamaño o sector, es así que varios países como Bermudas, Estados Unidos, Israel, Italia, Japón, Reino Unido, Suiza y Uruguay lo han adoptado como parte de su estrategia de ciberseguridad o de su legislación nacional.(Almagro, 2019)

La seguridad informática se ha vuelto esencial en las organizaciones en los últimos años debido a los grandes avances tecnológicos y la masificación del uso de dispositivos móviles en las actividades cotidianas mismas que van desde mensajería instantánea, compras y ventas en línea, control automatizado o remoto de hogares, teletrabajo a transacciones financieras. Debido a las amenazas informáticas a las que se encuentran expuestas las organizaciones y personas las cuales buscan secuestrar información delicada con el fin de solicitar rescate o uso fraudulento de la misma. Es aquí donde la seguridad informática se vuelve esencial tanto para empresas como personas, buscando los mecanismos más adecuados para salvaguardar la información dependiendo de cada realidad y concientizar a los usuarios de lo que afirma Guantiva-Acosta (2015) «la seguridad es responsabilidad de cada individuo y no solamente de las organizaciones».

Como lo manifiesta Parra (2019) en la actualidad la mayoría de empresas tanto públicas como privadas, basan en la información sus decisiones para lograr sus objetivos organizacionales y la

continuidad del negocio, lo cual la convierte en un activo esencial para las organizaciones al igual que las personas.

Debido que la información es el bien más preciado de toda institución, a la cantidad y criticidad de la información que se maneja en el Área de Sistematización de la Universidad Israel, se ve la necesidad de diseñar un esquema de seguridad informática esquema basado en la comparativa de la norma internacional ISO 27002 y el marco de Cybersecurity Framework del National Institute of Standards and Technology (CSF de NIST), bajo las políticas de seguridad que permita garantizar la integridad, disponibilidad y confidencialidad de la información. La principal finalidad es establecer directrices y principios de seguridad para mantener y mejorar la gestión de la seguridad en el Área.

Problema de investigación

Actualmente la Universidad Israel Tecnológica Israel cuenta con el área de Sistematización y Programación la cual es la responsable del desarrollo, mantenimiento y optimización de sistemas de información a medida, que permitan soportar los procesos cotidianos y críticos de la Universidad. Sin embargo, el área no cuenta con políticas de seguridad, controles, estándares y herramientas que permitan garantizar la integridad, disponibilidad y confidencialidad de la información.

Partiendo del principio típico en seguridad «lo no está permitido está prohibido, cada organización debería detectar las necesidades que le son específicas y valorar los controles necesarios que fundamenten las políticas aplicables, desarrollando la mejor estructura y relaciones entre ellas para su gestión más adecuada» (López & Ruiz, 2020).

La información como activo más importante de las empresas y falta de controles y salvaguardas en temas de seguridad de la información de las empresas han hecho que las organizaciones cibercriminales realicen ataques sofisticados y dirigidos con gran éxito logrando recaudar grandes sumas de dinero como rescate de la información comprometida.

La seguridad informática se logra por medio de implementación de los controles adecuados como políticas, procedimientos, procesos, funciones y estructuras organizacionales las cuales una vez implementadas deben ser revisadas y mejoradas con el fin de que estén alineadas con los objetivos organizacionales de seguridad y del negocio (UNE, 2017).

La información ha trascendido de letras, números e imágenes a formas intangibles como el conocimiento, conceptos, ideas y marcas. La información y sus procesos, sistemas informáticos, medios de comunicación y personal encargado de su manipulación y resguardo son activos que al igual que los activos importantes de la organización son valiosos y requieren implementar las respectivas salvaguardas ante las diversas amenazas y riegos. (UNE, 2017) .

La seguridad informática según Fernández et al. (2022) es el aliado perfecto para el cumplimiento de los objetivos y la misión de las organizaciones, mediante la protección de los recursos y activos más importantes como la información, tecnología que la soporta y personal encargado de su manejo y custodia mediante la definición e implementación de las medidas de protección adecuadas, que permitan mantener a salvo los activos tangibles e intangibles como la reputación.

El software cumple con un ciclo de vida como planificación, análisis, diseño, implementación, pruebas, instalación o despliegue, soporte y se debe considerar la seguridad informática en cada una de estas fases con el fin de detectar brechas de seguridad en las fases tempranas y evitar costos adicionales o rediseños de software y así lograr un producto final de calidad que genere valor para la organización.

Como sugiere Sánchez & Ramírez (2022) se debe incorporar requerimientos de seguridad a los requerimientos funcionales del software con el afán de identificar a tiempo cualquier amenaza que podrían convertirse en una vulnerabilidad en los sistemas. Un punto importante a considerar según UNE (2017) es que los nuevos desarrollo o cambios a sistemas actuales son oportunidades que la organización tiene para mejorar o actualizar los controles de seguridad tomado en cuenta incidencias reales y los riesgos de seguridad ligados a incidencias actuales y futuras.

Las entidades se ven en la necesidad de diseñar esquemas de seguridad de la información basado en normativas internacionales de buenas prácticas como la ISO 27002 y la CSF de NIST la cual permita que todos los colaboradores tengan claro que hacer y cómo hacerlo, mediante la definición de directrices y principios de seguridad para mantener y mejorar la gestión de la seguridad en el Área.

En el área es necesario definir principalmente Políticas de seguridad, control de Accesos que permita evitar el acceso no autorizado mediante la definición de privilegios, roles y perfiles de acuerdo al cargo que desempeña cada funcionario, además se debe restringir el acceso al código fuente para evitar robos, alteraciones, o la aplicación de ingeniería inversa por parte de personas no autorizadas,

y controles de seguridad en cada etapa de desarrollo de software que permitir minimizar vulnerabilidades y generar un producto de software de calidad.

De esta manera, se plantea la pregunta:
¿Cómo garantizar la integridad, confidencialidad y disponibilidad de la información del dominio de Políticas de Seguridad en el área de Sistematización Institucional de la Universidad Tecnológica Israel?

Objetivo general

Diseñar un esquema de seguridad informática para el área de Sistematización de la Universidad Israel basado en la comparativa de las normativa ISO 27002:2013 y CSF de NITS específicamente en el dominio de políticas de seguridad.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre buenas prácticas de seguridad de la información basado en las normas ISO 27002 y CSF de NIST para Instituciones de Educación Superior.
- Diagnosticar el estado actual de las políticas de seguridad de la información en la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, mediante la aplicación de las normas ISO 27002 y CSF de NIST, identificando el nivel de madurez basado en las métricas de COBIT 5, y la selección de la norma.
- Desarrollar un esquema de seguridad informática para la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, basado en el dominio de las políticas de seguridad aplicando la norma.
- Valorar mediante criterio de especialistas el esquema de seguridad informática basado en el dominio de políticas de seguridad de la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel.

Vinculación con la sociedad y beneficiarios directos:

Este trabajo tiene la finalidad de definir un modelo de políticas de seguridad de la información para el área de sistematización de la Universidad Tecnológica Israel con el fin de garantizar los pilares fundamentales de la integridad, confidencialidad y disponibilidad de la información y por ende los beneficiarios directos serian la comunidad Universitaria.

De acuerdo a los Objetivos de Desarrollo Sostenible adoptados por la ONU, el presente trabajo de investigación estaría dentro del objetivo número nueve “Industria, Innovación e Infraestructuras”. Ya que la definición de un esquema de seguridad informática permitirá que se optimicen procesos y se aplique las salvaguardas necesarias para la información.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

La seguridad de la información se logra mediante la implementación de controles adecuados, como políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware.

1.1. Contextualización general del estado del arte

Seguridad de la Información

Es el conjunto de políticas y medidas preventivas o reactivas que buscan salvaguardar la información de las entidades de los ataques cibernéticos, uso, divulgación y alteración no autorizada, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

La seguridad de la información abarca la protección tanto de los sistemas, recursos, información y activos ante el acceso o uso no autorizado, catástrofes o errores, con el fin de minimizar el riesgo y el impacto de los incidentes de seguridad de la información (Silva-Coelho et al., 2014).

Y como lo indica UNE (2017) «Los controles se deberían establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización».

La seguridad de la información abarca algunos conceptos importantes:

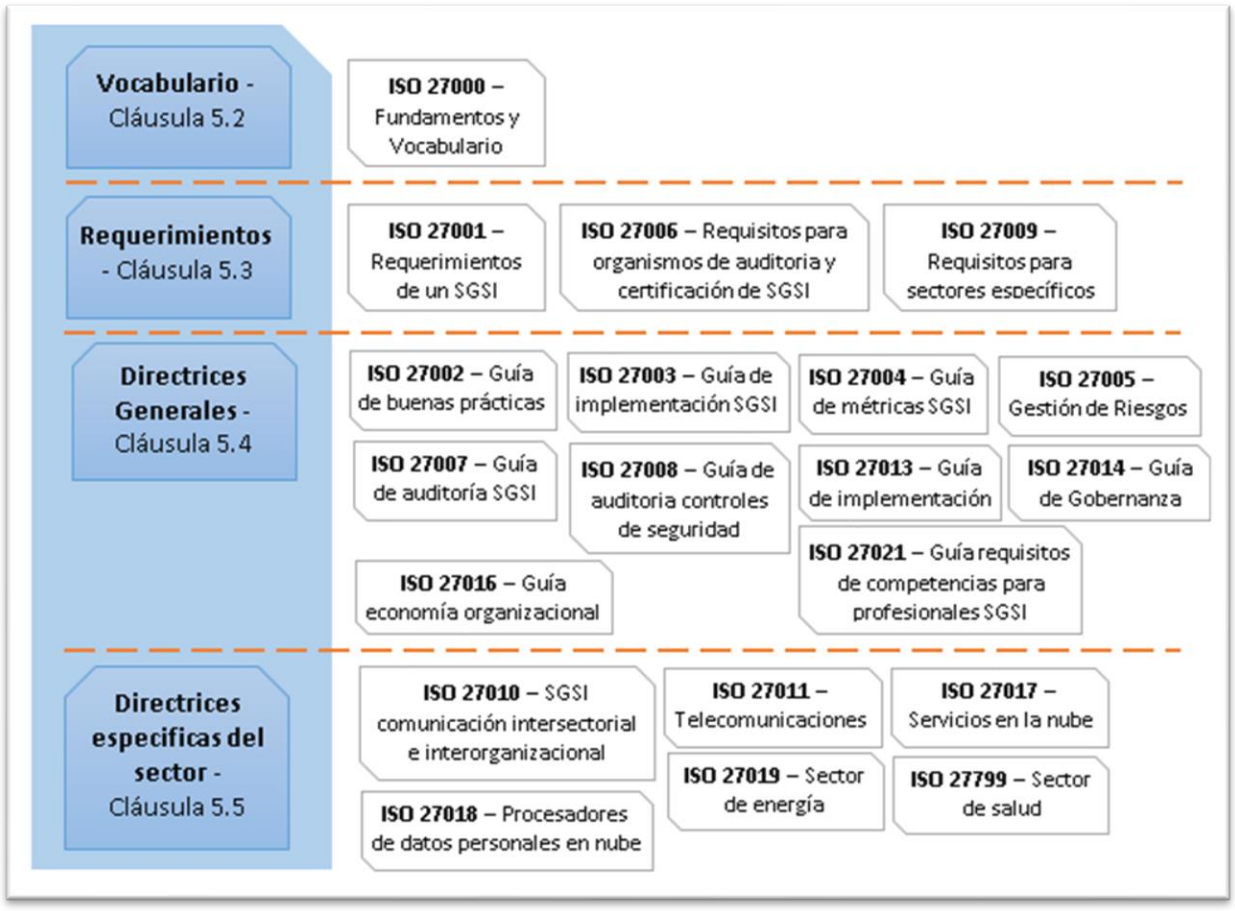
- **Activo**: todo elemento que represente valor para la entidad.
- **Amenaza**: cualquier evento o suceso que pueda generar un incidente no deseado que cause daño a un activo.
- **Vulnerabilidad**: cualquier debilidad en los activos de la información la cual pueda ser explotada y comprometa la seguridad del mismo.
- **Riesgo**: es la probabilidad de que una amenaza se materialice causando pérdidas o daños en los activos de la entidad.
- **Ataque**: cualquier evento que pueda comprometer la seguridad de una entidad.
- **Impacto**: es el resultado de materialización de una amenaza.

ISO 27000

La ISO 27000 es una familia de estándares interrelacionados para la gestión de seguridad de la información, desarrollado y publicado por la Organización Internacional de Normalización (ISO) y la

Comisión Electrotécnica Internacional (IEC), la única norma certificable es la ISO 27001, las demás son guías de buenas prácticas para la seguridad de la información. (ISO & IEC, 2018)

Figura 1.
Familia ISO 27000



Nota: Tomado de ISO/IEC 27000:2018

ISO 27002

Según lo especifica la norma ISO 27001:2013 La norma ISO 27002 anteriormente ISO 17799 es una normativa internacional para la seguridad de la información publicada por la organización internacional de normalización y la comisión electrotécnica internacional.

La norma ISO 27002 brinda diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para las empresas que deseen implementar o mantener sistemas de gestión de la seguridad de la información. Esta norma define a la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad. (ISOTools Excellence, 2017)

Estructura de la Normativa

La norma ISO 27002:2013 está conformada por:

- 14 Dominios
- 35 objetivos de control
- 114 controles

Figura 2.
Dominios ISO 27002:2013

Nota: Dominios ISO 27002:2013 basado en la fuente: https://www.unit.org.uy/normalizacion/sistema/27000/

Dominio de Políticas de Seguridad

El documento llamado política es donde la alta gerencia de la organización detalla explícitamente su posición y compromiso para garantizar la confidencialidad, integridad y disponibilidad de la información.

Como lo indica ISOTools Excellence (2017). El contenido de las políticas se fundamenta en el contexto de operación de la organización y contempla los objetivos de la organización, las estrategias adoptadas para lograr dichos objetivos, la estructura organizacional y los procesos propios de la organización. Es así que las políticas están ligadas estrechamente y se definen en base a los objetivos institucionales, de negocio y al entorno e incluso a un área específica de cada organización.

La Política de seguridad de la información es el documento base del cual se derivan el resto de políticas como desarrollo seguro, gestión de incidentes, etc. Además, es de los puntos

fundamentales para el cumplimiento de la ISO 27001 y describe de forma general las salvaguardas a tomarse con el fin de proteger los activos importantes de la organización, disminuir los riesgos e identificar posibles problemas y amenazas de seguridad. Dando como resultado un valor agregado a la organización como lo afirma Pirani (2019) incrementa la reputación organizacional, generar mayor seguridad, confianza y mejora las relaciones con los distintos grupos de interés, reduce y mitiga la materialización de riesgos tecnológicos.

Controles del Dominio de Políticas de Seguridad

El Domino de Política de Seguridad pose 2 controles:

5.1.1 Políticas para la seguridad de la información

5.1.2 Revisión de las políticas de seguridad de la información

Políticas para la seguridad de la información

En este punto debemos diferenciar entre la política que hace referencia a uno de los requisitos de la ISO 27001 la cual es un compromiso y las medidas que toma la alta gerencia para salvaguardar la información y las políticas específicas que son las que se abarcan en este control son más detallados y establecen lineamientos para el correcto manejo y protección de los activos de la organización, tal como lo manifiestan López & Ruiz (2020) es frecuente confundir el requisito de la Norma ISO 27001 en la cláusula 5.2 referente a la política de gestión del SGSI con el desarrollo de las políticas complementarias las cuales contemplan la implantación practica de controles a nivel operativo del tratamiento de la información por parte de usuarios, sistemas y plataformas.

> Los desarrollos de las políticas específicas deben establecer los controles en función de los objetivos de la organización o área, las estrategias, la estructuras y procesos, normativas legales que le rijan y el sector al que pertenece la organización. (López & Ruiz, 2020)

Las políticas deben ser aprobadas por la alta gerencia, deben publicarse y comunicarse a todo el personal de organización en todo nivel incluso a externos y no únicamente a nivel de directivos y responsables.

Las políticas deben ser revisadas y actualizada periódicamente para que se adapten a los cambios y necesidades de la empresa y a las nuevas amenazas cibernéticas con el fin de conseguir sus objetivos organizacionales y garantizar el resguardo de los activos más importantes.

Las políticas de seguridad de la información especificas se definen en función de los dominios, objetivos y controles de la norma ISO 27002:2013.

Formato de las políticas especificas

Las políticas específicas deberían considerar las siguientes secciones:

Tabla 1.
Secciones de política específica

Sección	Descripción
Historial de revisión	Historial de cambios con versión, fecha, responsable y observación.
Revisión y aprobación	Firmas de responsables de elaborar, revisar y aprobara la política.
Objetivo	Identificar el por qué requiere la creación de la política de seguridad de información.
Alcance	Define a que áreas, procesos o departamentos se aplica la política y quienes deben cumplirla.
Referencias	Normas a las cuales hace referencia la política.
Definiciones	Definición de términos propios de la política.
Roles y responsabilidades	Define los responsables y sus roles para el cumplimiento de la política
Política	Descripción de los controles y lineamientos a tomarse para dicho control de la política.
Periodicidad de evaluación y revisión	Periodicidad establecida para la evaluación y revisión de cumplimiento de la política.
Difusión	Determina el medio por el cual será definida y su vigencia.

Nota: Elaboración propia

Revisión de las políticas de seguridad de la información

Las políticas de la seguridad de la información deben ser dinámicas y por ende revisadas y evaluadas periódicamente, cuando se identifican riesgos o si ocurren cambios significativos en la organización como la misión, objetivos, infraestructura o personal, todo esto con el fin de que las políticas de adapten a la nueva realidad de la organización y así garantizar aptas y efectivas. Como lo describe normaiso27001.es (2019) «Las políticas de la Seguridad de la información deben adaptarse continuamente a las necesidades y cambios de la organización por lo que no pueden permanecer estáticas».

NIST Cybersecurity Framework (CSF)

El Cybersecurity Framework (CSF) es un marco de ciberseguridad para la protección de infraestructuras criticas el cual fue desarrollado por el Instituto de Nacional de Estándares y Tecnologías (NIST) de Estados Unidos, su versión inicial fue emitida en 2014 y su la actualización a la versión 1.1 se publicó en 2018. (Almagro, 2019)

El CFS es una recopilación de lineamientos y mejores prácticas en un lenguaje común para la ciberseguridad, es flexible, adaptable y busca crear o complementar el programa de ciberseguridad de una organización independientemente del sector o tamaño, cuyo objetivo es que las organizaciones comprendan, gestionen y reduzcan los riesgos cibernéticos y protejan sus redes y datos. (NIST, 2018)

El CFS permite a las organizaciones identificar y priorizar las salvaguardas que le permitan minimizar el riesgo cibernético mediante la alineación de sus políticas, negocios y tecnología, y como lo expresa NIST (2018) “se puede utilizar para administrar el riesgo de seguridad cibernética en todas las partes de una organización o se puede enfocar en la entrega de servicios críticos dentro de una parte de la organización”.

Estructura del Cybersecurity Framework (CSF)

El CSF está enfocado en minimizar el riesgo vinculado a las amenazas cibernéticas, y está formado por 3 partes principales:

Framework Core: «es el conjunto de actividades, resultados deseados y referencias aplicables de la ciberseguridad los cuales son comunes en los sectores de infraestructura critica». (NIST, 2018)

El Framework Core consta de cuatro elementos:

- **Funciones**: columna vertebral del Framework Core
    - **Identificar ID**: Identifica los activos y procesos críticos de la organización para priorizar las salvaguardas para las áreas críticas.
    - **Proteger PR**: Desarrolla las salvaguardas priorizando las áreas más críticas.
    - **Detectar DE**: Desarrolla controles que permitan detectar oportunamente eventos de ciberseguridad.
    - **Responder RS**: conjunto de medidas para hacer frente a un ataque se ciberseguridad detectado para mitigar el impacto.

- **Recuperar RC**: conjunto de controles del plan de residencia que permiten recuperar la operación normal luego de un incidente de ciberseguridad.

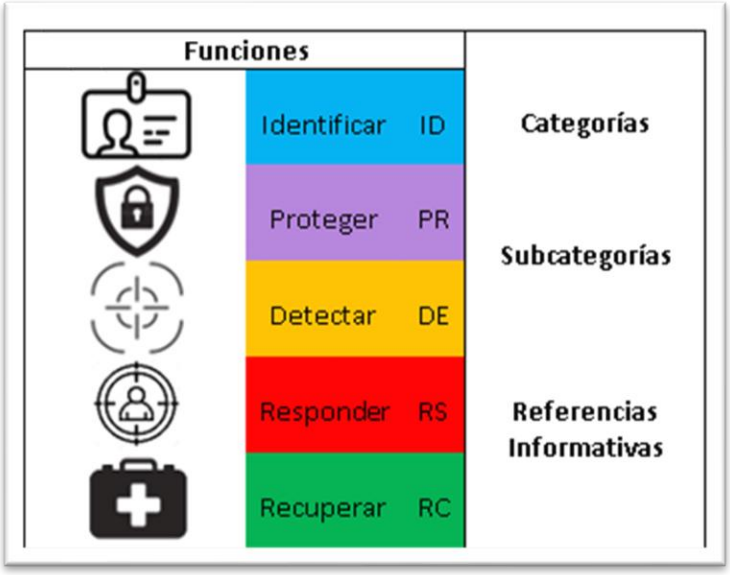
- **Categorías**: son 23 subdivisiones de las funciones que agrupan los resultados de actividades específicas como Gestión de Activo, Procesos de Detección, etc.

- **Subcategorías**: son 108 divisiones de las categorías representan los resultados de actividades técnicas o de gestión y respaldan los logros de cada Categoría.

- **Referencias Informativas**: son normas, prácticas y directrices comunes que proveen una metodología para lograr los resultados de cada Subcategoría.

Figura 3.

Elementos del Framework Core



Nota: Elaboración propia

Niveles de Implementación: representan en qué grado de madurez o el nivel deseado en cuanto a la gestión de riesgos de ciberseguridad desea implementar la organización, conforme a los objetivos organizacionales. (García, 2020)

Se definen 4 niveles del más básico al más robusto:

- **Nivel 1: Parcial** los lineamientos de la gestión de riesgos de ciberseguridad no están formalizados y se ejecuta de forma reactiva.

- **Nivel 2: Riesgo Informado** las medidas de gestión del riesgo están aprobadas por la alta dirección por no se han definido políticas para toda la organización.

- **Nivel 3: Repetible** las medidas para gestión del riesgo se encuentran formalizadas en políticas y se actualizan periódicamente conforme a las amenazas, tecnología y objetivos organizaciones.

- **Nivel 4: Adaptativo** las medidas de gestión de riesgo de ciberseguridad se actualizan periódicamente en base a lecciones aprendidas, amenazas actuales y predicciones.

Cada uno de los niveles considera los atributos de Proceso de Gestión de Riesgos, Programa Integrado de Gestión de Riesgos y Participación externa

Figura 4.

Niveles de Implementación CFS

Nota. Elaboración propia

Perfil: determina la situación actual de la gestión de seguridad cibernética de la organización y al compararla con el perfil objetivo desarrollar un plan de acción que permita gestionar brechas y mejoras.

Modelo de Madurez COBIT 5

COBIT es un marco de trabajo enfocado en las tecnologías de información (TI) que ayuda a las organizaciones a comprender el gobierno y la gestión de las tecnologías de información (TI), y evaluar en qué estado se encuentran las TI en la empresa.

Como lo manifiesta Ramírez (2018) «Es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control» y mediante evoluciones fáciles concientizar y motivar a la mejora a las organizaciones .

Los modelos de madurez permiten a las organizaciones medir la capacidad y madurez de los distintos procesos.

Niveles de Clasificación de la madurez

COBIT utiliza los siguientes niveles de clasificación de la madurez con una escala de 0 a 5

Tabla 2.
Niveles de madurez COBIT

Nivel		Descripción
Inexistente	**0**	No se aplican procesos, La organización no ha identificado un problema a resolver.
Inicial	**1**	La organización ha identificado un problema a resolver pero no ha estandarizado un proceso, solo procesos ad-hoc y desorganizados.
Repetible	**2**	Los procesos siguen un patrón regular, no hay capacitación o comunicación formal del proceso y la responsabilidad se deja a la persona.
Definida	**3**	Los procedimientos no son sofisticados sino practicas existentes que han sido estandarizados, documentados y comunicados mediante la capacitación. El seguimiento del proceso se ha dejado en manos de la persona.
Administrada	**4**	Los procesos son monitoreados, medidos y en constante mejora. Se usa automatización y herramientas de forma limitada.
Optimizada	**5**	Se aplica mejores prácticas, se integra la automatización y herramientas para mejora la calidad y efectividad.

Nota: Elaboración propia basado en COBIT modelo de madurez

1.2. Proceso investigativo metodológico

La investigación fue mediante un enfoque metodológico cualitativo, donde se utilizó la investigación descriptiva e interpretativa, basado en la revisión documental, además para fortalecer la investigación se utilizó la técnica e instrumento de entrevista, aplicado al director y programadores de la Unidad de Sistematización Institucional sobre dominios, objetivos de control y controles de

seguridad de la información, en base a la norma ISO 27002:2013 y CSF de NITS, con el fin de mitigar los posibles ataques y amenazas de seguridad de la información.

Población

La población en la presente investigación está conformada por todos los miembros de la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, donde son los responsables de la seguridad de la información automatizada.

Muestra

La muestra en la presente investigación se ha tomado en cuenta a los responsables directos o principales de Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, que están conformado por:

- 1 director
- 1 jefe de programadores
- 1 programador

Revisión documental

En este proceso de revisión documental se analizó la normativa interna (políticas, procesos y procedimientos) que posee la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, en referencia a la seguridad de la información. Para ello se tomó en cuenta los dominios, objetivos de control y controles de seguridad de la información, en base a la norma ISO 27002:2013 y CSF de NITS.

Como lo manifiesta (Martín & Lafuente, 2017) la revisión documental es la etapa fundamental para la elaboración de todo trabajo académico o científico, el cual consistente en buscar y recuperar documentos de diversa fuentes de información como papers, tesis, revistas, catálogos, bases de datos, repositorios.

Entrevista

La entrevista fue elaborada en base a instrumentos ya validados y aplicados en otras investigaciones, mismo que adicionalmente fue consultada con el tutor de la presente investigación.

Se tomó en cuenta para dicha elaboración los dominios, objetivos de control y controles de seguridad de la información, en base a la norma ISO 27002:2013 y CSF de NITS, cómo se establece a continuación:

Figura 5.
Formato Entrevista

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS

La presente entrevista tiene el fin de conocer la opinión de los responsables directos o principales de Unidad de Sistematización Institucional de la Universidad Tecnológica Israel. La información recabada permitirá levantar el nivel de madurez de la seguridad de la información en base a la norma ISO 27002:2013 y CSF de NITS

Datos informativos

Nombre del entrevistado:
C.I.:
Cargo:
Años de experiencia en el área:

Preguntas:

Políticas de seguridad	¿Cuenta la Unidad de Sistematización Institucional con manuales de Políticas de seguridad de la información?
	¿Las políticas de Seguridad de la información se encuentran aprobada, publicadas y comunicadas al personal?
	¿ Existe un proceso periódico de revisión y actualización de las políticas para que se adapten a los cambios y necesidades de la Unidad?
Aspectos Organizativos de la	¿Se han asignado responsabilidades de políticas de seguridad de la información dentro de la Unidad?

Página 1 de 9

Nota: Elaboración propia

1.3. Análisis de resultados

En base al análisis de los resultados obtenidos tanto en la revisión documental como en las entrevistas, se determinó el nivel de madurez basado en las métricas de COBIT 5. Adicionalmente, por el análisis y resultados obtenidos, se seleccionó la norma ISO 27002:2013 para desarrollar el esquema de seguridad de la información en la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel.

Revisión Documental

Por temas de sigilo de la información recibida por parte de la Unidad de Sistematización Institucional, no se puede evidenciar detalles específicos en la presente investigación, pero fue tomada en cuenta para la valoración del nivel de madurez.

Entrevistas

Se desarrolló las 3 entrevistas planteadas en la muestra, de las cuales se obtuvieron los siguientes resultados:

Tabla 3.
Resultados Entrevista

Pregunta ¿Cuenta la Unidad de Sistematización Institucional con manuales de Políticas de seguridad de la información?
Análisis: 
Pregunta ¿Las políticas de Seguridad de la información se encuentran aprobadas, publicadas y comunicadas al personal?
Análisis: 
Pregunta ¿Existe un proceso periódico de revisión y actualización de las políticas para que se adapten a los cambios y necesidades de la Unidad?
Análisis: 
Pregunta ¿Se han asignado responsabilidades de políticas de seguridad de la información dentro de la Unidad?
Análisis: 
Pregunta ¿La Unidad de Sistematización cuenta con un área encargada de la seguridad de la información?
Análisis: 
Pregunta ¿En la Unidad se ha contratado personal con conocimientos de seguridad de la información?
Análisis: 
Pregunta ¿Al realizar contratos con empresas externas exige cláusulas de seguridad de la información?
Análisis: 
Pregunta ¿Cuenta con políticas y procedimientos para el acceso de dispositivos móviles?
Análisis: 
Pregunta ¿Cuenta con controles para el acceso remoto por motivos de teletrabajo?
Análisis: 
Pregunta ¿Cuenta con una política de control de acceso basada en los requisitos de negocio y de seguridad de la información?
Análisis: 
Pregunta ¿Cuenta con un procedimiento para el registro y baja de usuarios?

Análisis: 

Pregunta ¿Cuenta con procedimientos para la gestión de asignación o revocatoria de los derechos de acceso?

Análisis: 

Pregunta ¿Maneja roles con derechos de accesos privilegiados?

Análisis: 

Pregunta ¿Cuenta con políticas y procedimientos para la gestión de la información confidencial de autenticación de usuarios?

Análisis: 

Pregunta ¿Existe un manejo adecuado de la información confidencial de autenticación como contraseña y llaves criptográficas?

Análisis: 

Pregunta ¿Existen procedimientos seguros de inicio de sesión?

Análisis: 

Pregunta ¿Existe un procedimiento formal en cuanto a la gestión de contraseñas, su robustez, cambio periódico y almacenamiento?

Análisis: 

Pregunta ¿Manejan un control del acceso al código fuente de los programas?

Análisis: 

Pregunta ¿Se incluyen requisitos de seguridad de la información en los requisitos de desarrollo de nuevos sistemas o mejoras de sistemas de información?

Análisis: 

Pregunta ¿Cuenta con medidas de protección que garanticen la confidencialidad, la integridad y el origen de los datos en las transacciones por redes telemáticas?

Análisis: 

Pregunta ¿Usan normas de desarrollo seguro en nuevos desarrollos o actualizaciones de los sistemas informáticos?

Análisis: 

Pregunta ¿Cuenta con procedimientos formales de control de cambios en el software?

Análisis: 

Pregunta ¿Se hace uso de principios de ingeniería en protección de sistema para cualquier labor de implementación en los sistemas de información?

Análisis: 

Pregunta ¿Cuenta con procedimientos de desarrollo seguro?

Análisis: 

Pregunta ¿Cuenta con procedimientos para la supervisión y control del desarrollo de software externalizado?
Análisis: 

Pregunta ¿Realizan pruebas funcionales de seguridad durante el desarrollo de los sistemas?
Análisis: 

Pregunta ¿Usan enmascaramiento de datos u otros controles de seguridad para la información de los datos de pruebas?
Análisis: 

Nota: Elaboración propia

Nivel de madurez (ISO 27002:2013 y CSF de NITS)

A partir de la revisión documental realizada a la normativa de la Universidad Tecnológica Israel, se determinó el nivel de madurez de la seguridad de la información de la Unidad de Sistematización Institucional, basado en las métricas de COBIT 5 y aplicando una comparativa de las normas ISO 27002:2013 y CSF de NITS, obteniendo los resultados de dominios, objetivos de control y controles de seguridad de la información.

Los porcentajes asignados para cada nivel de madurez COBIT se obtuvo mediante la proporcionalidad directa tomando en cuenta que al nivel más alto con valor cinco se le asigna el porcentaje de cien por ciento.

Matriz de nivel de madurez mapeo ISO 27002:2013 y CSF de NIST

Tabla 4.
Matriz de Calificación de Madurez COBIT

Nivel	Valor	Descripción	Documentación	Monitoreo	Proceso	%
Inexistente	**0**	No se aplican procesos, La organización no ha identificado un problema a resolver.	-	-	-	0%
Inicial	**1**	La organización ha identificado un problema a resolver pero no ha estandarizado un proceso, solo procesos ad-hoc y desorganizados.	Divulgado	-	-	36%
Repetible	**2**	Los procesos siguen un patrón regular, no hay capacitación o comunicación formal del proceso y la responsabilidad se deja a la persona.	No formal	-	-	40%
Definida	**3.5**	Los procedimientos no son sofisticados sino practicas existentes que han sido estandarizados, documentados y comunicados mediante la capacitación.	Formal	No	-	70%
	3.8	El seguimiento del proceso se ha dejado en manos de la persona.	Formal	Si	-	76%
Administrada	**4.25**	Los procesos son monitoreados, medidos y en constante mejora.	Formal	Si	Manual	85%
	4.75	Se usa automatización y herramientas de forma limitada.	Formal	Si	Semiautomático	95%
Optimizada	**5**	Se aplica mejores prácticas, se integra la automatización y herramientas para mejora la calidad y efectividad.	Formal	Si	Automático	100%

Nota: Elaboración propia basado en COBIT modelo de madurez

Tabla 5.
Matriz de Madurez en base al Mapeo ISO 27002:2013 y CSF de NIST

ISO 27002:2003		CSF de NIST		
Control	**Descripción**		**%**	**Descripción**
A.5	**Políticas de seguridad.**		**#,##%**	
5.1	**Directrices de la Dirección en seguridad de la información.**		CONFIDENCIAL	
A.5.1.1	Conjunto de políticas para la seguridad de la información	ID.GV-1, ID.GV-2	CONFIDENCIAL	
A.5.1.2	Revisión de las políticas para la seguridad de la información		CONFIDENCIAL	
A.6	**Aspectos organizativos de la seguridad de la información**		**#,##%**	
6.1	**Organización interna**		CONFIDENCIAL	
A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	ID.AM-6, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, DE.DP-1, RS.CO-1	CONFIDENCIAL	
A.6.1.2	Segregación de tareas.	PR.AC-4, PR.DS-5, RS.CO-3	CONFIDENCIAL	
A.6.1.3	Contacto con las autoridades.	RS.CO-2	CONFIDENCIAL	
A.6.1.4	Contacto con grupos de interés especial.	ID.RA-2, RS.CO-5, RC.CO-1	CONFIDENCIAL	
A.6.1.5	Seguridad de la información en la gestión de proyectos.	PR.IP-2	CONFIDENCIAL	
6.2	**Dispositivos para movilidad y teletrabajo.**		CONFIDENCIAL	
A.6.2.1	Política de uso de dispositivos para movilidad.	PR.AC-3, PR.AC-3	CONFIDENCIAL	
A.6.2.2	Teletrabajo		CONFIDENCIAL	
A.7	**Seguridad ligada a los recursos humanos.**		**#,##%**	
7.1	**Antes de la contratación.**		CONFIDENCIAL	
A.7.1.1	Investigación de antecedentes.	PR.AC-6, PR.DS-5, PR.IP-11		
A.7.1.2	Términos y condiciones de contratación.	PR.DS-5, PR.IP-11	CONFIDENCIAL	
7.2	**Durante la contratación.**		CONFIDENCIAL	
A.7.2.1	Responsabilidades de gestión.	ID.GV-2, PR.AT-3, PR.IP-11		
A.7.2.2	Concienciación, educación y capacitación en segururidad de la información.	PR.AT-1, PR.AT-2,	CONFIDENCIAL	

		PR.AT-3, PR.AT-4, PR.AT-5, PR.IP-11, DE.DP-1, RS.CO-1	
A.7.2.3	Proceso disciplinario.	PR.IP-11	CONFIDENCIAL
7.3	**Cese o cambio de puesto de trabajo.**		CONFIDENCIAL
A.7.3.1	Cese o cambio de puesto de trabajo.	PR.DS-5, PR.IP-11	
A.8	**Gestión de activos.**		**#,##%**
8.1	**Responsabilidad sobre los activos.**		CONFIDENCIAL
A.8.1.1	Inventario de activos.	ID.AM-1	
A.8.1.2	Propiedad de los activos	ID.AM-1	CONFIDENCIAL
A.8.1.3	Uso aceptable de los activos		
A.8.1.4	Devolución de activos.	PR.IP-11	CONFIDENCIAL
8.2	**Clasificación de la información.**		
A.8.2.1	Directrices de clasificación.	ID.AM-5, PR.PT-2	CONFIDENCIAL
A.8.2.2	Etiquetado y manejo de información	PR.DS-5, PR.PT-2	CONFIDENCIAL
A.8.2.3	Manipulación de activos.	PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-5, PR.IP-6, PR.PT-2	CONFIDENCIAL
8.3	**Manejo de los soportes de almacenamiento.**		CONFIDENCIAL
A.8.3.1	Gestión de soportes extraíbles.	PR.DS-3, PR.IP-6, PR.PT-2	CONFIDENCIAL
A.8.3.2	Eliminación de soportes.	PR.DS-3, PR.IP-6	CONFIDENCIAL
A.8.3.3	Soportes físicos en tránsito.	PR.DS-3, PR.PT-2	CONFIDENCIAL
A.9	**Control de accesos.**		**#,##%**
9.1	**Requisitos de negocio para el control de accesos.**		CONFIDENCIAL
A.9.1.1	Política de control de accesos.	PR.DS-5	
A.9.1.2	Control de acceso a las redes y servicios asociados.	PR.AC-4, PR.DS-5, PR.PT-3	CONFIDENCIAL
9.2	**Gestión de acceso de usuario.**		
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	PR.AC-1, PR.AC-6, PR.AC-7	CONFIDENCIAL
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	PR.AC-1	CONFIDENCIAL

A.9.2.3	Gestión de los derechos de acceso con privilegios especiales.	PR.AC-1, PR.AC-4, PR.DS-5	CONFIDENCIAL
A.9.2.4	Gestión de información confidencial de autenticación de usuarios.	PR.AC-1, PR.AC-7	CONFIDENCIAL
A.9.2.5	Revisión de los derechos de acceso de los usuarios.		CONFIDENCIAL
A.9.2.6	Retirada o adaptación de los derechos de acceso	PR.AC-1	CONFIDENCIAL
9.3	**Seguridad de los equipos**		CONFIDENCIAL
A.9.3.1	Uso de información confidencial para la autenticación.	PR.AC-1, PR.AC-7	
9.4	**Control de acceso a sistemas y aplicaciones.**		CONFIDENCIAL
A.9.4.1	Restricción del acceso a la información.	PR.AC-4, PR.DS-5	CONFIDENCIAL
A.9.4.2	Procedimientos seguros de inicio de sesión.	PR.AC-1, PR.AC-7	CONFIDENCIAL
A.9.4.3	Gestión de contraseñas de usuario.	PR.AC-1, PR.AC-7	CONFIDENCIAL
A.9.4.4	Uso de herramientas de administración de sistemas.	PR.AC-4, PR.DS-5	CONFIDENCIAL
A.9.4.5	Control de acceso al código fuente de los programas.	PR.AC-4, PR.DS-5	CONFIDENCIAL
A.10	**Cifrado**		**#,##%**
10.1	**Política de uso de los controles criptográficos.**		CONFIDENCIAL
A.10.1.1	Política de control de accesos.	PR.DS-5	CONFIDENCIAL
A.10.1.2	Gestión de claves.		
A.11	**Seguridad física y ambiental**		CONFIDENCIAL
11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física.	PR.AC-2, DE.CM-2	CONFIDENCIAL
A.11.1.2	Controles físicos de entrada.	PR.AC-2, PR.MA-1, DE.CM-2	CONFIDENCIAL
A.11.1.3	Seguridad de oficinas, despachos y recursos.	PR.AC-2	CONFIDENCIAL
A.11.1.4	Protección contra las amenazas externas y ambientales.	ID.BE-5, PR.AC-2, PR.DS-5	
A.11.1.5	El trabajo en áreas seguras.	PR.AC-2, PR.DS-5	CONFIDENCIAL
A.11.1.6	Áreas de acceso público, carga y descarga.	PR.AC-2	CONFIDENCIAL
11.2	Seguridad de los equipos		
A.11.2.1	Emplazamiento y protección de equipos.	PR.AC-2, PR.DS-5, PR.IP-5	CONFIDENCIAL
A.11.2.2	Instalaciones de suministro.	ID.BE-4, PR.IP-5	CONFIDENCIAL

A.11.2.3	Seguridad del cableado	ID.BE-4, PR.AC-2, PR.IP-5	CONFIDENCIAL
A.11.2.4	Mantenimiento de los equipos	PR.DS-8, PR.MA-1, PR.MA-2	CONFIDENCIAL
A.11.2.5	Salida de activos fuera de las dependencias de la empresa.	PR.AC-2, PR.DS-3, PR.MA-1	CONFIDENCIAL
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	ID.AM-4, PR.AC-2, PR.AC-3, PR.MA-1	CONFIDENCIAL
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	PR.AC-2, PR.DS-3, PR.IP-6	CONFIDENCIAL
A.11.2.8	Equipo informático de usuario desatendido.	PR.AC-2	CONFIDENCIAL
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	PR.PT-2	
A.12	**Seguridad en la operativa.**		**#,##%**
12.1	**Responsabilidades y procedimientos de operación**		CONFIDENCIAL
A.12.1.1	Documentación de procedimientos de operación.	DE.AE-1	CONFIDENCIAL
A.12.1.2	Gestión de cambios.	PR.IP-1, PR.IP-3, DE.AE-1	CONFIDENCIAL
A.12.1.3	Gestión de capacidades.	ID.BE-4, PR.DS-4	CONFIDENCIAL
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	PR.DS-7	CONFIDENCIAL
12.2	**Protección contra código malicioso.**		CONFIDENCIAL
A.12.2.1	Controles contra el código malicioso.	PR.AT-1, PR.DS-6, DE.CM-4, RS.MI-1, RS.MI-2	
12.3	**Copias de seguridad**		CONFIDENCIAL
A.12.3.1	Copias de seguridad de la información.	PR.IP-4	
12.4	**Registro de actividad y supervisión.**		CONFIDENCIAL
A.12.4.1	Registro y gestión de eventos de actividad.	PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-3, DE.CM-7, RS.AN-1	
A.12.4.2	Protección de los registros de información.	PR.PT-1	CONFIDENCIAL
A.12.4.3	Registros de actividad del administrador y operador del sistema.	PR.PT-1, DE.CM-3, RS.AN-1	
A.12.4.4	Sincronización de relojes.	PR.PT-1	CONFIDENCIAL

12.5	**Control del software en explotación**		CONFIDENCIAL
A.12.5.1	Instalación del software en sistemas en producción.	PR.DS-6, PR.IP-1, PR.IP-3, DE.CM-5	
12.6	**Gestión de la vulnerabilidad técnica**		CONFIDENCIAL
A.12.6.1	Gestión de las vulnerabilidades técnicas.	ID.RA-1, ID.RA-5, PR.IP-12, DE.CM-8, RS.MI-3	
A.12.6.2	Restricciones en la instalación de software.	PR.IP-1, PR.IP-3, DE.CM-5	CONFIDENCIAL
12.7	**Consideraciones de las auditorías de los sistemas de información.**		CONFIDENCIAL
A.12.7.1	Controles de auditoría de los sistemas de información.	PR.PT-1	CONFIDENCIAL
A.13	**Seguridad en las telecomunicaciones.**		**#,##%**
13.1	**Gestión de la seguridad en las redes**		CONFIDENCIAL
A.13.1.1	Controles de red.	PR.AC-3, PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-4, DE.AE-1	
A.13.1.2	Mecanismos de seguridad asociados a servicios en red.	DE.AE-1	CONFIDENCIAL
A.13.1.3	Segregación de redes.	PR.AC-5, PR.DS-5	CONFIDENCIAL
13.2	**Intercambio de información con partes externas**		CONFIDENCIAL
A.13.2.1	Políticas y procedimientos de intercambio de información.	ID.AM-3, PR.AC-3, PR.AC-5, PR.DS-2, PR.DS-5, PR.PT-4	CONFIDENCIAL
A.13.2.2	Acuerdos de intercambio.	ID.AM-3	CONFIDENCIAL
A.13.2.3	Mensajería electrónica.	PR.DS-2,PR.DS-5	CONFIDENCIAL
A.13.2.4	Acuerdos de confidencialidad y secreto.	PR.DS-5	CONFIDENCIAL
A.14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		**#,##%**
14.1	**Requisitos de seguridad de los sistemas de información.**		CONFIDENCIAL
A.14.1.1	Análisis y especificación de los requisitos de seguridad.	PR.IP-2	CONFIDENCIAL

A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	PR.AC-5, PR.DS-2, PR.DS-5, PR.DS-6	CONFIDENCIAL
A.14.1.3	Protección de las transacciones por redes telemáticas.	PR.AC-5, PR.DS-2, PR.DS-5, PR.DS-6, PR.PT-4	CONFIDENCIAL
14.2	**Seguridad en los procesos de desarrollo y soporte**		CONFIDENCIAL
A.14.2.1	Política de desarrollo seguro de software.	PR.IP-2	CONFIDENCIAL
A.14.2.2	Procedimientos de control de cambios en los sistemas.	PR.IP-1, PR.IP-3	CONFIDENCIAL
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	PR.IP-1, PR.IP-3, PR.IP-12	CONFIDENCIAL
A.14.2.4	Restricciones a los cambios en los paquetes de software.	PR.DS-6, PR.IP-1, PR.IP-3	CONFIDENCIAL
A.14.2.5	Uso de principios de ingeniería en protección de sistemas.	PR.IP-2	CONFIDENCIAL
A.14.2.6	Seguridad en entornos de desarrollo.		CONFIDENCIAL
A.14.2.7	Externalización del desarrollo de software.	DE.CM-6, DE.CM-7	CONFIDENCIAL
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	DE.DP-3	CONFIDENCIAL
A.14.2.9	Pruebas de aceptación.		CONFIDENCIAL
14.3	Datos de prueba		CONFIDENCIAL
A.14.3.1	Protección de los datos utilizados en pruebas.		CONFIDENCIAL
A.15	**Relaciones con suministradores.**		**#,##%**
15.1	**Seguridad de la información en las relaciones con suministradores**		CONFIDENCIAL
A.15.1.1	Política de seguridad de la información para suministradores.	ID.BE-1, ID.GV-2, ID.SC-1, ID.SC-3, PR.MA-2	CONFIDENCIAL
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	ID.BE-1, ID.SC-1, ID.SC-3	CONFIDENCIAL
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	ID.BE-1, ID.SC-1, ID.SC-3	CONFIDENCIAL
15.2	Gestión de la prestación del servicio por suministradores		CONFIDENCIAL
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros.	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-4,	CONFIDENCIAL

		PR.MA-2, DE.CM-6, DE.CM-7	
A.15.2.2	Gestión de cambios en los servicios prestados por terceros.	ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-4	
A.16	**Gestión de incidentes en la seguridad de la información**		**#,##%**
16.1	**Gestión de incidentes de seguridad de la información y mejoras.**		
A.16.1.1	Responsabilidades y procedimientos.	PR.IP-9, DE.AE-2, RS.CO-1	
A.16.1.2	Notificación de los eventos de seguridad de la información.	DE.DP-4	
A.16.1.3	Notificación de puntos débiles de la seguridad.	PR.IP-12	
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	DE.AE-2, DE.AE-4, DE.AE-5, RS.AN-2, RS.AN-4	
A.16.1.5	Respuesta a los incidentes de seguridad.	RS.RP-1, RS.AN-1, RS.MI-1, RS.MI-2, RC.RP-1	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	ID.RA-4, PR.IP-7, PR.IP-8, DE.DP-5, RS.AN-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-2	
A.16.1.7	Recopilación de evidencias.	DE.AE-1, RS.AN-3	
A.17	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**		**#,##%**
17.1	**Continuidad de la seguridad de la información**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	ID.BE-5, PR.IP-9	
A.17.1.2	Implantación de la continuidad de la seguridad de la información.	ID.BE-5, PR.IP-4, PR.IP-9, PR.PT-5	

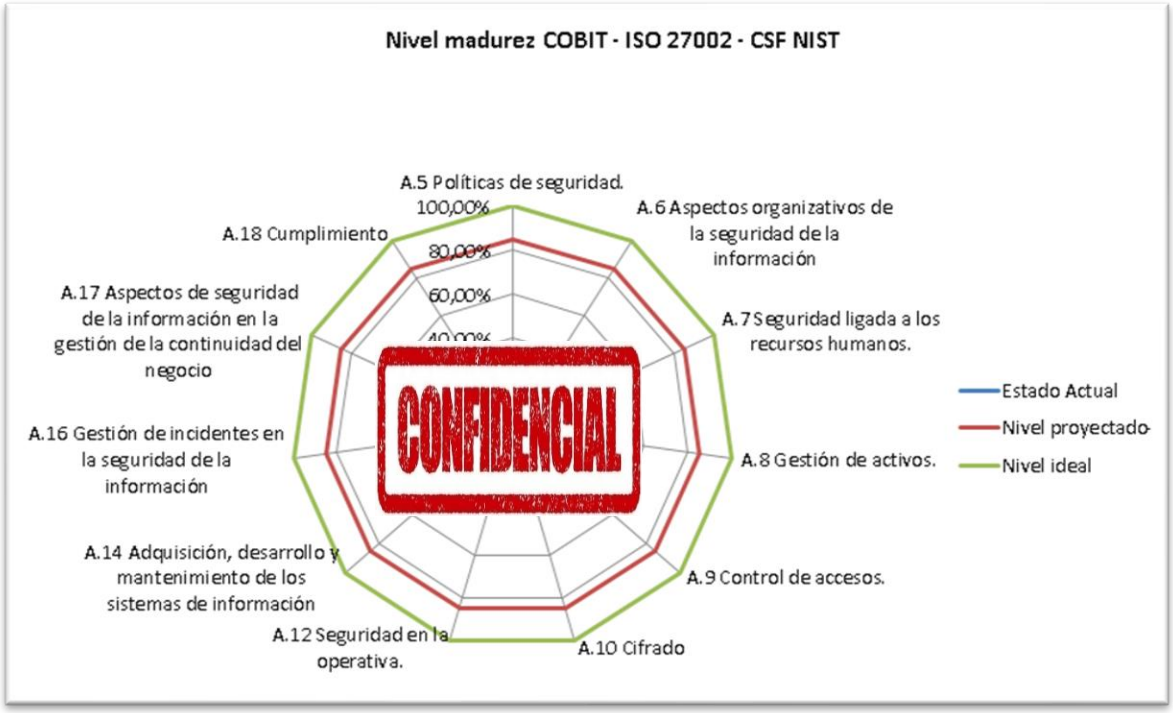
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	ID.SC-1, PR.IP-4, PR.IP-9, PR.IP-10	
17.2	**Redundancias.**		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	ID.BE-5, PR.DS-4, PR.PT-5	
A.18	**Cumplimiento**		**#,##%**
18.1	**Cumplimiento de los requisitos legales y contractuales**		
A.18.1.1	Identificación de la legislación aplicable.	ID.GV-3	
A.18.1.2	Derechos de propiedad intelectual (DPI).	ID.GV-3	
A.18.1.3	Protección de los registros de la organización.	ID.GV-3, PR.IP-4	
A.18.1.4	Protección de datos y privacidad de la información personal.	ID.GV-3, PR.AC-7, DE.DP-2	
A.18.1.5	Regulación de los controles criptográficos.	ID.GV-3	
18.2	**Revisiones de la seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información.		
A.18.2.2	Cumplimiento de las políticas y normas de seguridad.	PR.IP-12, DE.DP-2	
A.18.2.3	Comprobación del cumplimiento.	ID.RA-1, PR.IP-12, DE.DP-2	

Nota: Elaboración propia basado en ISO 27002:2013 y CSF de NIST

Figuras de resultados

Figura 6.

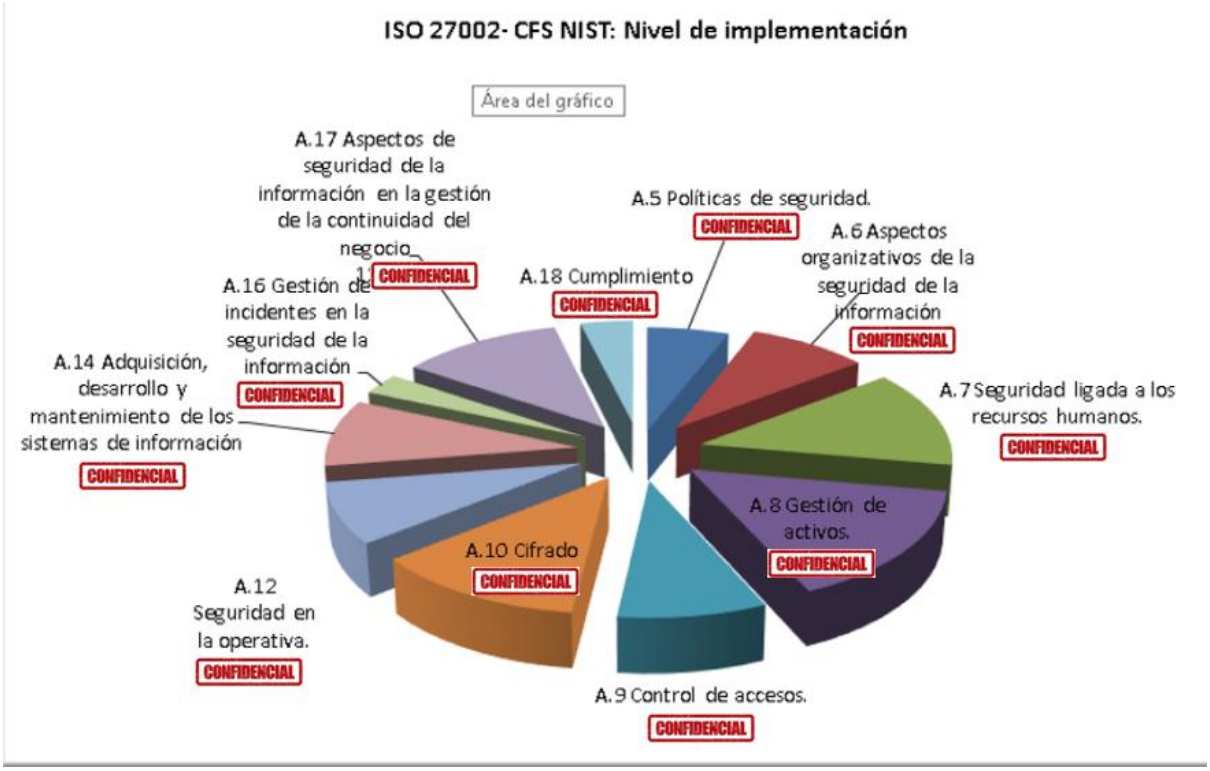
Nivel de Madurez ISO 27002:2013 y CSF de NIST



Nota: Elaboración propia

Figura 7.

Nivel de Implementación ISO 27002:2013 y CSF de NIST



Nota: Elaboración propia

CAPÍTULO II: PROPUESTA

Este capítulo se enfoca en la propuesta de un esquema de seguridad de la información, basado en los resultados obtenidos en la evaluación de madurez de la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, con respecto a los dominios, objetivos de control y controles de la Norma ISO 27002:2013.

2.1 Fundamentos teóricos aplicados

Para la presente investigación se analizó la Norma ISO 27002:2013 y el CSF de NIST, mismas que consisten en un conjunto de mejores prácticas para la ciberseguridad, del cual, por los resultados obtenidos y aplicabilidad a la universidad, se considerará solamente la norma ISO 27002:2013, ya que adicionalmente ofrece una mayor cobertura respecto al CSF de NIST. A su vez, en el futuro la universidad puede optar por la certificación ISO 27001, ya que la ISO 27002 es el anexo A de la Norma ISO 27001.

Figura 8.

Niveles de cobertura Frameworks y Normativas

Nota: Niveles de Cobertura Frameworks y Normativas. (2020). https://www.complianceforge.com/products/

Como complianceforge (2020) lo especifica la norma ISO 27002:2013 es un subconjunto de la NIST 800-53 abarcando 14 secciones y controles de seguridad de 20 familias de la NIST 800-53 rev5; por otro lado, el CSF de NIST incorpora partes de la ISO 27002 y de NIST 800-53, por lo cual su cobertura es menor lo cual no le permitiría cubrir los requerimientos de Payment Card Industry Data Security Standard (PCI DSS) .

Dominio Políticas de seguridad

Las políticas específicas que se abarcan en este domino son más detalladas y establecen lineamientos para el correcto manejo y protección de los activos de la organización y deben establecer los controles en función de los objetivos de la organización o área, las estrategias, la estructuras y procesos, normativas legales que le rijan y el sector al que pertenece la organización (López-Neira & Ruiz-Spohr, 2020)

Las políticas de seguridad especificas se desarrollan en base a los dominios, objetivos de control y controles de la Norma ISO 27002:2013

Modelo de Madurez COBIT 5

El marco de trabajo COBIT maneja un modelo de madurez permite a las organizaciones medir la capacidad de madurez de sus procesos. El cual maneja una escala que va de 0 a 5 el cual muestra como un proceso va evolucionando desde inexistente a optimizado, se utiliza en el presente trabajo para determinar el nivel de madurez del Área de Sistematización en base a la implementación dominios, objetivos de control y controles de la ISO 27002.

2.2 Descripción de la propuesta

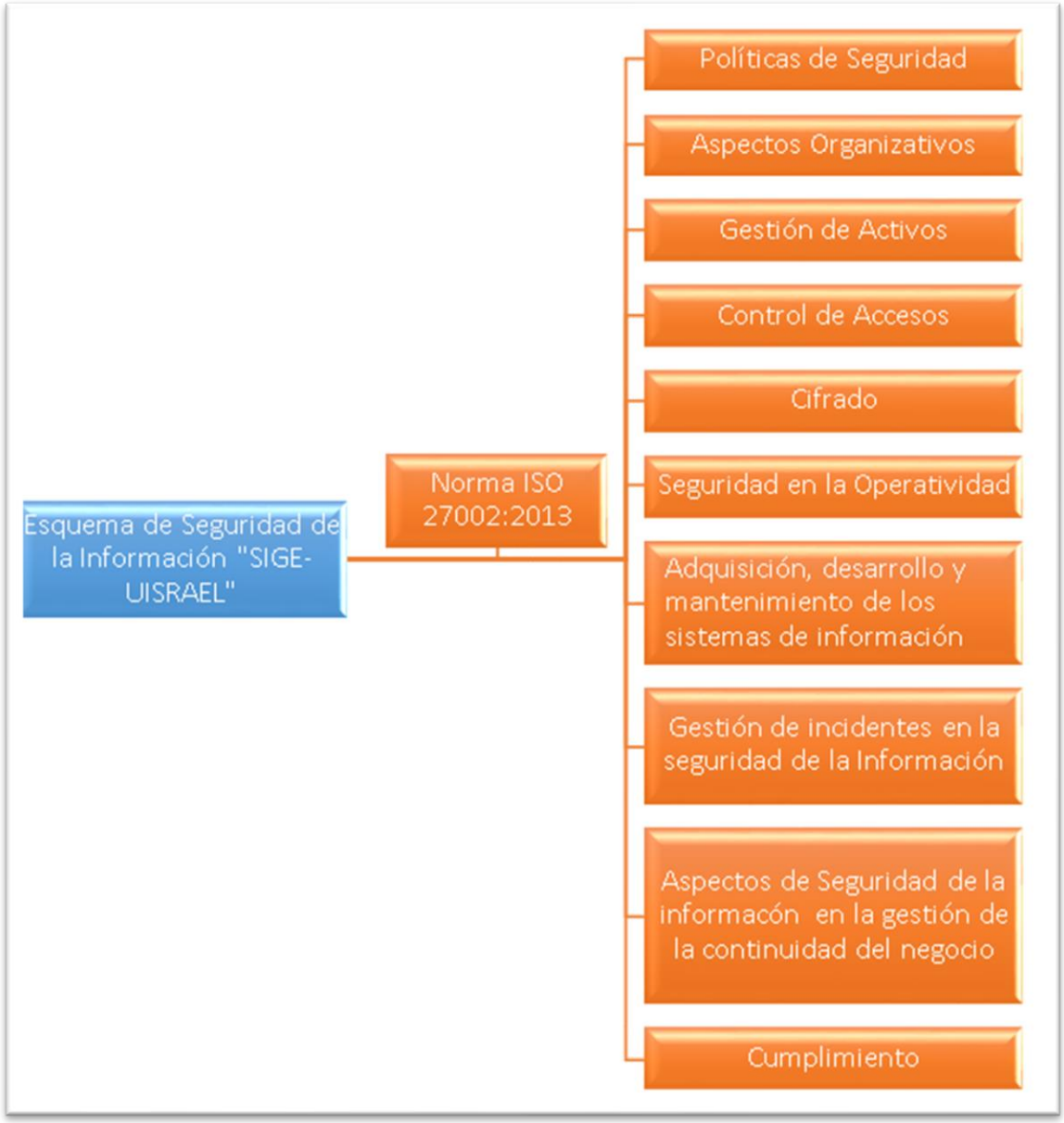
Se desarrolló un esquema de seguridad de la información, tomando en cuenta la evaluación de madurez de la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel, con respecto a los dominios, objetivos de control y controles de la Norma ISO 27002:2013.

a. Estructura general

Basado en la propuesta del esquema de seguridad de la información se posee la siguiente estructura:

Figura 9.

Esquema General de la propuesta



Nota: Elaboración propia

b. Explicación del aporte

De acuerdo a los dominios del esquema de seguridad de la información propuesto, a continuación, se especifica las acciones a tomar en cuenta por cada objetivo de control y controles del mismo.

Políticas de Seguridad

Dominio	Objetivo de control	Control	Propuesta
5. Políticas de seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información 5.1.2 Revisión de las políticas para la seguridad de la información	
6. Aspectos Organizativos Seguridad de la Información	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la Seguridad de la Información 6.1.2 Segregación de tareas	
		6.1.3 Contacto con las autoridades 6.1.5 Seguridad de la información en la gestión de proyectos	
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad 6.2.2 Teletrabajo	
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	
		8.1.2 Propiedad de los activos	
		8.1.3 Uso aceptable de los activos	

		8.1.4 Devolución de activos	
	8.2 Clasificación de la información	8.2.1 Directrices de clasificación	
		8.2.2 Etiquetado y manipulado de la información	
		8.2.3 Manipulación de activos	
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles	
		8.3.2 Eliminación de soportes	
9. Control de Accesos	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos	
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios	
		9.2.2 Gestión de los derechos de acceso asignados a usuarios	
		9.2.3 Gestión de los derechos de acceso con privilegios especiales	
		9.2.4 Gestión de información confidencial de autenticación de usuarios	
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación	

	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información 9.4.2 Procedimientos seguros de inicio de sesión 9.4.3 Gestión de contraseñas de usuario 9.4.5 Control de acceso al código fuente de los programas	
10. Cifrado	10.1 Controles criptográficos	10.1.1 Política de uso de los controles criptográficos 10.1.2 Gestión de claves:	
12. Seguridad en la Operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación 12.1.2 Gestión de cambios 12.1.4 Separación de entornos de desarrollo, prueba y producción	
	12.2 Protección contra código malicioso 12.3 Copias de seguridad	12.2.1 Controles contra el código malicioso 12.3.1 Copias de seguridad de la información	

	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad	
		12.4.2 Protección de los registros de información	
		12.4.3 Registros de actividad del administrador y operador del sistema	
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción	
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas	
		12.6.2 Restricciones en la instalación de software	
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información	
14. Adquisición, desarrollo y Mantenimiento de los sistemas de información	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad	
	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro de software	
		14.2.2 Procedimientos de control de cambios en los sistemas	
		14.2.6 Seguridad en entornos de desarrollo	
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	

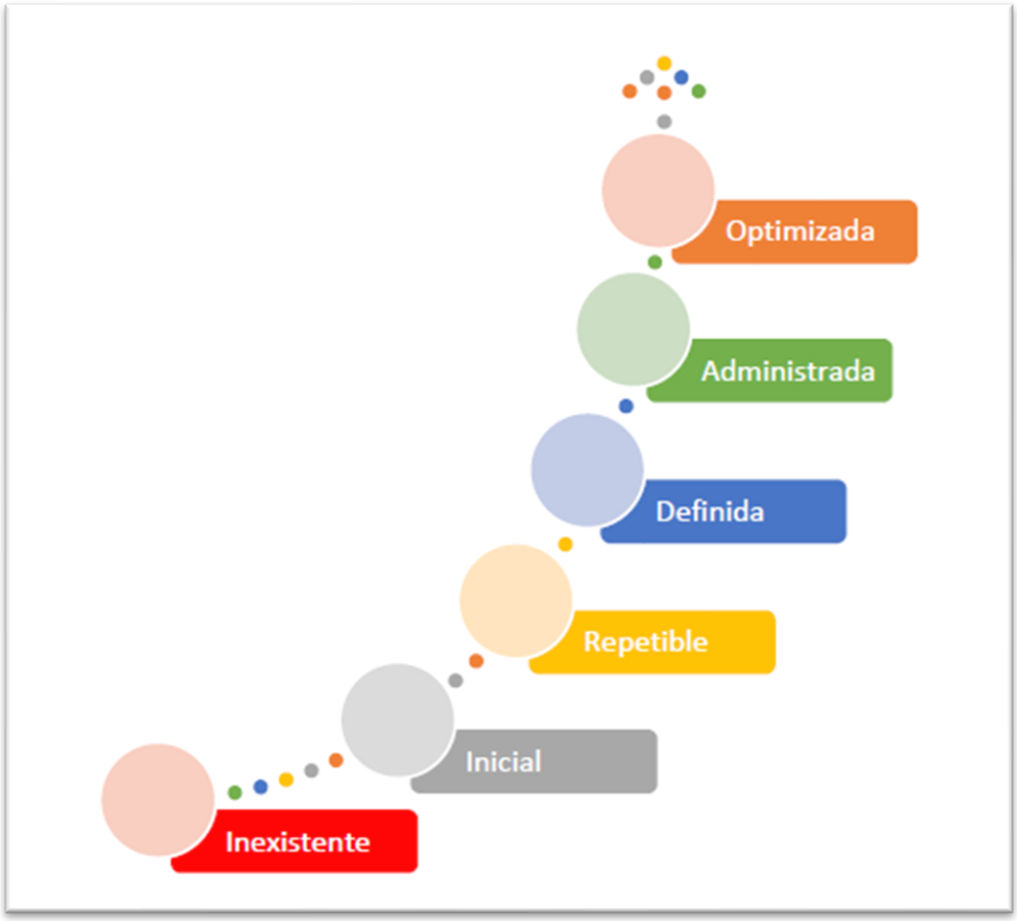
		14.2.9 Pruebas de aceptación
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en prueba
16. Gestión de Incidentes	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones 16.1.5 Respuesta a los incidentes de seguridad 16.1.6 Aprendizaje de los incidentes de seguridad de la información 16.1.7 Recopilación de evidencias
17. Aspectos de la Seguridad de la Información en la Gestión de la Continuidad de Negocio	17.2 Redundancias	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1 Identificación de la legislación aplicable 18.1.2 Derechos de propiedad intelectual (DPI) 18.1.4 Protección de datos y privacidad de la información personal
	18.2.3 Comprobación del cumplimiento	18.2.3 Comprobación del cumplimiento

c. Técnicas

La presente propuesta considera como técnicas para la evaluación del nivel de madurez de la seguridad de información, a las métricas de COBIT 5.

Figura 10.

Niveles de Madurez COBIT 5

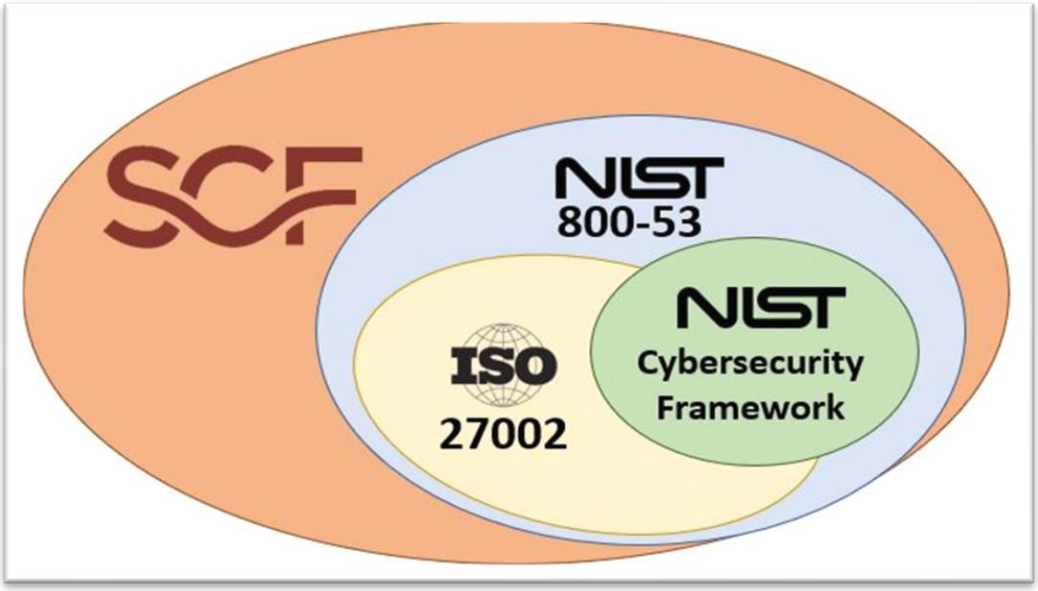


Nota: Elaboración propia basado en COBIT 5

Adicionalmente, como parte de la fundamentación científica de seguridad de la información se tomó en cuenta a las normas ISO 27002:2013 y CSF de NITS.

Figura 11.

Comparativa SCF , NIST 800-53, ISO 27002, NIST CSF



Nota: Comparativa SCF , NIST 800-53, ISO 27002, NIST CSF. (2020).
https://www.complianceforge.com/products/

2.3 Valoración de la propuesta

El esquema de seguridad diseñado para la Unidad de Sistematización Institucional de la Universidad Israel en base al nivel de madurez e implementación de la seguridad de la información respecto al mapeo de las normas ISO 27002:2013 y el CSF de NIST, permite establecer una guía de los dominios a ser implementados con el fin fortalecer la seguridad informática de la misma.

La presente propuesta fue valorada a través del método de criterios de especialistas, los cuales son profesionales en el área de seguridad de la información y con una experiencia mayor a 5 años, obteniendo los siguientes resultados.

De acuerdo con la valoración de los especialistas la presente propuesta es aplicable y factible, como expresa el especialista seguir los principios de una norma ISO/IEC 27002 es un paso altamente relevante para garantizar la seguridad de la información en las instituciones, como observación de uno de los especialistas indica que es necesario fortalecer la fundamentación teórica sobre el caso de estudios en universidades.

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, técnicos y tecnológicos empleados.

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Seguridad de la Información	Definición de Seguridad de la Información.	La metodología de investigación fue revisión documental que permitió tener los conceptos detallados	Fuente bibliográfica	Sustenta conocimientos previos requeridos para entender la propuesta	Texto, Figuras e Imágenes
ISO 27002:2013	La norma internacional ISO 27002:2013 es un conjunto de buenas prácticas para la seguridad de la información de cualquier organización, con el fin de minimizar el impacto ante ataques cibernéticos.	La metodología de investigación fue revisión documental que permitió tener los conceptos detallados	Fuente bibliográfica	Proporciona un conjunto de directrices y principios para implementar, mantener y mejorar la gestión de la seguridad de la información. Mapeo de la normativa ISO 27002:2013 y CSF de NIST.	Texto, Figuras e Imágenes, matrices
CSF de NIST	El Cyber Security Framework (CSF) de NIST, es un marco de ciberseguridad que consta de un	La metodología de investigación fue revisión documental	Fuente bibliográfica	Proporciona un conjunto de directrices y principios para implementar, mantener y mejorar la	Matrices

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
	conjunto de directrices para proteger la infraestructura critica, fue desarrollo por Estados Unidos en el 2014	que permitió tener los conceptos detallados.		gestión de la seguridad de la información. Mapeo de la normativa ISO 27002:2013 y CSF de NIST.	
COBIT 5	Modelo de madurez que contempla una escala que va de 0 a 5 el cual muestra como un proceso va evolucionando desde inexistente a optimizado	La metodología de investigación fue revisión documental que permitió tener los conceptos detallados.	Fuente bibliográfica	Se genera matriz de madurez de la Unidad de Sistematización Institucional del a Universidad Israel respecto al mapeo de la norma ISO 27002:2013 y CSF de NIST	Matriz de madurez , asignación de nivel de madurez según mapeo de la norma ISO:27002:2013 y CSF de NIST

CONCLUSIONES

La contextualización de los fundamentos teóricos sobre buenas prácticas de seguridad de la información como las normas ISO 27002 y CSF de NIST, permitió tener una radiografía general sobre las directrices, medidas y salvaguardas que se deben tomar en cuenta para garantizar la integridad, confidencialidad y disponibilidad de la información.

El diagnóstico del estado actual de las políticas de seguridad de la información basado en comparativa de la norma ISO 27002:2013 y CSF de NIST permitió determinar las fortalezas, debilites y nivel de madurez de la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel y definir a la norma ISO 27002:2023 como la directriz para el presente proyecto.

Los resultados del diagnóstico realizado fue el insumo principal para el desarrollo del esquema de seguridad informática basado en el dominio de las políticas de la norma ISO 27002:2013, para la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel.

La valoración a través de especialistas ayudo para fortalecer y validar la factibilidad del esquema de seguridad informática propuesto, mismo que la Universidad Tecnológica Israel implementará de acuerdo a su necesidad.

El diseño del esquema de seguridad basado en la norma ISO 27002:2013 nos dada una idea clara de que dominios debemos implementar, con el fin de que la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel fortalezca la seguridad de la información, para garantizar su integridad, confidencialidad y disponibilidad.

RECOMENDACIONES

Para el desarrollo de un proyecto de investigación sobre la temática planteada, es recomendable realizar inicialmente una revisión bibliográfica, ya que permite tener un panorama claro y los lineamientos sobre la norma ISO 27002:2013 y CSF de NIST y sus principios de la seguridad de la información.

Se recomienda realizar el diagnóstico sobre la situación actual, mediante un análisis comparativo de normas o marcos de seguridad de la información, con el fin de determinar el más adecuado y que se adapte a las necesidades y objetivos institucionales, haciendo énfasis en su cobertura y madurez.

Se recomienda definir las políticas y procedimientos para la Unidad de Sistematización Institucional de la Universidad Israel especialmente en los dominios A6 Aspectos organizativos de la seguridad de la información, A9 Control de accesos, A14 Adquisición, desarrollo y mantenimiento de los sistemas de información, las cuales permitirán asegurar la integridad, confidencialidad y disponibilidad en la sistematización de los procesos institucionales.

La valoración de especialistas es un pilar fundamental para medir el nivel de factibilidad y confiabilidad de la presente propuesta, por el cual se recomienda que para este tipo de proyectos siempre se lo realice.

Se recomienda que todos los procedimientos de la Unidad de Sistematización Institucional de la Universidad Israel sean documentados, aprobados, publicados y comunicados a todo el personal, se planifique su revisión y actualización periódica con el fin de garantizar que los mismos se encuentren alineados a los objetivos institucionales, sean adecuados y efectivos.

BIBLIOGRAFÍA

Almagro, L. (2019). *MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad*. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

complianceforge. (2020). *NIST 800-53 vs ISO 27002 vs NIST CSF*. https://www.complianceforge.com/grc/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf

García, A. (2020). *GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO*. https://z0jde8nnyvm1b6dkizyjcq.on.drv.tw/Publico/www.A-Garcia.edu/Mod11-GITI-GCN/2_framework_de_ciberseguridad_nist.html

Gavidia, J. (2022). Modelo de seguridad informática en el control de accesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NIST. http://repositorio.uisrael.edu.ec/handle/47000/3360

Guantiva Acosta, J. (2015). *La Cotidianidad de la Seguridad informática*. http://repository.unipiloto.edu.co/handle/20.500.12277/2789

ISO, & IEC. (2018). *ISO/IEC 27000:2018*. https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf

ISOTools Excellence. (2017, agosto 3). *Norma ISO 27002: El dominio política de seguridad*. https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

López Neira, A., & Ruiz Spohr, J. (2020, septiembre). *Iso27000*. iso27000.es. https://www.iso27000.es/iso27000.html

Martín, S. G., & Lafuente, V. (2017). Referencias bibliográficas: Indicadores para su evaluación en trabajos científicos. *Investigación Bibliotecológica: archivonomía, bibliotecología e información*, *31*(71), Article 71. https://doi.org/10.22201/iibi.0187358xp.2017.71.57814

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

normaiso27001.es. (2019). ISO 27002 punto a punto—A5 Políticas de Seguridad de la Información. *ISO 27001*. https://normaiso27001.es/a5-politicas-de-seguridad-de-la-informacion/

Parra Enríquez, J. P. (2019). *Diseño de políticas en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001 dirigidoa una empresa de equipos de telecomunicaciones.* http://repositorio.ug.edu.ec/handle/redug/46708

Pirani. (2019). *Guía para hacer una Política de Seguridad de la Información*. https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion

Ramírez, I. (2018, junio 6). *COBIT®—Modelo de Madurez*. iPMOGuide. https://ipmoguide.com/cobit-modelo-de-madurez/

Reinoso, D. (2017) Propuesta de sistema de gestión de seguridad de la información con la norma ISO/IEC 27001 – 27002 ver. 2013, para el Departamento de Sistemas y Recursos Tecnológicos de la Universidad Israel. http://repositorio.uisrael.edu.ec/handle/47000/1472

Silva, E. (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. http://repositorio.uisrael.edu.ec/handle/47000/3365

Silva Coelho, F., Segadas de Araújo, L. G., & Kowask Bezerra, E. (2014). *Gestión de la seguridad de la información*. RENATA. https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

UNE. (2017). *UNE-EN ISO/IEC 27002:2017*. https://www.industriaconectada40.gob.es/difusion/Paginas/enlaces-interes.aspx

Zapata, L. M. I., & Ríos, V. A. G. (2019). *Estado de la norma técnica de seguridad ISO27002 como soporte para la norma*. https://dspace.tdea.edu.co/bitstream/handle/tda/499/Estado%20de%20la%20norma%20tecnica%20de%20seguridad.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXO 1

VALORACIÓN DE ESPECIALISTAS

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALORACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Mg. Paúl Baldeón Egas
Título obtenido: Magister en Tecnologías
C.I.: 1002807814
E-mail: paulfrancisco_17@hotmail.com
Institución de Trabajo: Universidad Israel
Cargo: Director de Sistematización Institucional
Años de experiencia en el área: 15 años

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta del esquema de seguridad informática diseñado en base a la norma ISO 27002:2013 para la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad		X			
Fundamentación teórica		X			
TOTAL					

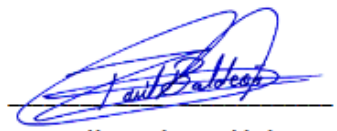
Observaciones:

Insuficiente fundamentación teórica sobre el caso de estudios en universidades, y por ende se posee una novedad que pudiese fortalecerse.

Recomendaciones:

Se puede fortalecer la fundamentación teórica con base a un proceso sistemático

Lugar, fecha de validación: .....



MSc. Paúl Francisco Baldeón Egas

Página **2** de **2**

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALORACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: ING. ROBERTO SANTIAGO PORTILLA PROAÑO

Título obtenido: INGENIERIA EN SISTEMAS COMPUTACIONALES

C.I.: 1002433058

E-mail: robertsan21@yahoo.es

Institución de Trabajo: COOPERATIVA DE AHORRO Y CREDITO ATUNTAQUI LTDA.

Cargo: ADMINISTRADOR DE SEGURIDAES INFORMATICAS

Años de experiencia en el área: 12 AÑOS

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta del esquema de seguridad informática diseñado en base a la norma ISO 27002:2013 para la Unidad de Sistematización Institucional de la Universidad Tecnológica Israel.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	x				
Aplicabilidad	x				
Factibilidad	x				
Novedad		x			
Fundamentación teórica	x				
TOTAL					

Observaciones: Es importante establecer métricas y coberturas en las políticas o directrices institucionales, que permitan definir el porcentaje de secciones de las normas ISO aplicables para las cuales se han especificado, escrito, aprobado y publicado, así como los procedimientos y procedimientos asociados, con el uso de sistemas automatizados lo cual permitirá mejorar y mantener estos esquemas fortaleciendo la seguridad de la información en todos sus pilares.

Recomendaciones: Seguir los principios de una certificación ISO/IEC 27002 es un paso altamente relevante para garantizar la seguridad de la información en las instituciones. En este sentido, es primordial resaltar la importancia de empresas en contar con profesionales certificados en sus equipos de seguridad, dando mayor respaldo al proceso de implementación de las buenas prácticas relacionadas a la norma de tal forma que se re afirmen los compromisos y mejoras en todos los procesos.

Lugar, fecha de validación: Ibarra, 20 de septiembre del 2023.

Firmado digitalmente por Santiago Portilla
Fecha: 2023.09.20 16:33:57 -05'00'

Ing. Roberto Santiago Portilla Proaño

ANEXO 2

FORMATO DE ENTREVISTA

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

DISEÑO DE UN ESQUEMA DE SEGURIDAD INFORMÁTICA PARA EL ÁREA DE SISTEMATIZACIÓN DE LA UNIVERSIDAD ISRAEL, APLICANDO ISO 27002 y CSF de NITS

La presente entrevista tiene el fin de conocer la opinión de los responsables directos o principales de Unidad de Sistematización Institucional de la Universidad Tecnológica Israel. La información recabada permitirá levantar el nivel de madurez de la seguridad de la información en base a la norma ISO 27002:2013 y CSF de NITS

Datos informativos

Nombre del entrevistado:

C.I.:	
Cargo:	
Años de experiencia en el área:	

Preguntas:

Políticas de seguridad	¿Cuenta la Unidad de Sistematización Institucional con manuales de Políticas de seguridad de la información?
	¿Las políticas de Seguridad de la información se encuentran aprobada, publicadas y comunicadas al personal?
	¿ Existe un proceso periódico de revisión y actualización de las políticas para que se adapten a los cambios y necesidades de la Unidad?
Aspectos Organizativos de la	¿Se han asignado responsabilidades de políticas de seguridad de la información dentro de la Unidad?

seguridad de la información	¿La Unidad de Sistematización cuenta con una área encargada de la seguridad de la información?
	¿En la Unidad se ha contratado personal con conocimientos de seguridad de la información?
	¿Al realizar contratos con empresas externas exige cláusulas de seguridad de la información?
	¿Cuenta con políticas y procedimientos para el acceso de dispositivos móviles?
	¿Cuenta con controles para el acceso remoto por motivos teletrabajo?
Seguridad Ligada a los recursos humanos	¿cuenta con procesos para la investigación de antecedentes de los contratistas y candidatos a un puesto de trabajo?
	¿Cuenta con un código de ética y conducta, compromiso de confidencialidad y no revelación para los contratos de trabajo?
	¿Cuenta con políticas, procedimientos y controles de seguridad de la información para determinar las responsabilidades de empleados y contratistas?
	¿Cuenta con un programa de capacitación y concienciación del personal en temas se políticas y procedimientos organizaciones les de acuerdo a sus puestos de trabajo?
	¿cuenta con un proceso disciplinario formal que haya sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad?
	¿Cuenta con procedimientos para el cese de funciones o cambio de puesto de trabajo ?
	¿Se cuenta con un inventario de activos de información actualizado?
Gestión Activos	¿cuenta con controles para la asignación de activos y sus responsabilidades?
	¿cuenta con cláusulas o convenios de responsabilidad respecto al uso aceptable de los activos de información?

	¿cuenta con proceso de desvinculación que incluya la devolución de todo activo físico y electrónico que sean propiedad de la organización o estén bajo su custodia?
	¿Cuenta con un procedimiento de clasificación de la información?
	Cuenta con procedimientos para el etiquetado y manipulación de la información?
	¿¿cuenta con procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.?
	¿Cuenta con procedimientos y niveles de autorización para gestión de los soportes extraíbles?
	¿Posee procedimientos formales para la eliminación de soporte de forma segura?
	¿cuenta con procedimientos para el transporte de soportes físicos que permitan su protección accesos no autorizados, usos indebidos o deterioro?
	¿Cuenta con una política de control de acceso basada en los requisitos de negocio y de seguridad de la información?
Control de Accesos	¿El acceso a las redes y servicios en red lo realizan solo los usuarios autorizados?
	¿Cuenta con un procedimiento para el registro y baja de usuarios?
	¿Cuenta con procedimientos para la gestión de asignación o revocatoria los derechos de acceso?
	¿Maneja roles con derechos de acceso privilegiados?
	¿Se consideran los principios de menor privilegio y segregación de funciones en la gestión de derechos de acceso?
	¿Maneja Acuerdos de confidencialidad?
	¿Cuenta con Revisiones periódicas de los derechos de acceso o cuando existe una promoción o cambio de cargo del usuario?
	¿Cuenta con un procedimiento formal para la gestión de eliminación o adaptación de derechos de acceso?

	¿Existe un manejo adecuado de la información confidencial de autenticación como contraseña y llaves criptográficas?
	¿Cuenta con autenticación de doble factor?
	¿Existen restricciones de acceso a la información?
	¿Existen procedimientos seguros de inicio de sesión?
	¿existe un procedimiento formal en cuanto a la gestión de contraseñas, su robustez, cambio periódico y almacenamiento?
	¿Hacen uso de herramientas de administración de sistemas capaces de anular o evitar controles en aplicaciones?
	¿ Manejan un control del acceso al código fuente de los programas?
Cifrado	¿La Unidad de Sistematización Institucional cuenta con políticas de uso de controles criptográficos?
Seguridad física y Ambiental	¿cuenta con instalaciones físicas para el manejo de información sensible o crítica?
	¿Se dispone de algún sistema de seguridad física contra desastres naturales, ataques maliciosos o accidentes en las instalaciones de la Unidad?
	¿manejar procedimientos para trabajo en áreas seguras?
	¿Existe un control de las áreas a las cuales es permitido el acceso a personal no autorizado?
	¿Se cuenta con controles para minimizar el riesgo de posibles amenazas físicas y ambiéntale en los equipo?
	¿se pose procedimientos o controles en cuanto a las áreas de suministros y redundancia de electricidad, telecomunicaciones?
	¿cuenta con controles en cuanto al manejo e instalación de cableado eléctrico y de comunicaciones?
	¿ Cuenta con procedimientos formales para la gestión de mantenimiento y relación de los equipos?
	¿Cuenta con controles para la gestión de salida de equipos portátiles que manejen o almacenen información organizacional fuera de la Universidad?

	¿Cuenta con procedimientos de eliminación segura de información sensible de dispositivos de almacenamiento?
	¿Cuenta con políticas que permitan progre el acceso no autorizado cuando un equipo se encuentra desatendido mente bloqueo automático o contarles equivalentes?
Seguridad en la Operativa	¿Los procedimientos operativos de la Unidad se encuentra debidamente documentados (gestión de pistas de auditoria, copias de seguridad, procesos de monitoreo)?
	¿Cuentan con un procedimientos formales que permitan gestionar y llevar un control de cambios de procesos o sistemas de tratamiento de la información?
	¿Cuenta con controles que permitan identificar y gestionar los requisitos de capacidad de los recursos y sistemas de misión critica?
	¿Cuenta con procedimientos para segregación de entornos de desarrollo, pruebas y operación?
	¿Cuenta con controles que permitan detectar, prevenir y recuperarse ante ataques de código malicioso?
	¿Cuentan con procedimientos de capacitación y concienciación para el personal?
	¿Cuentan con políticas de respaldo para las copias de seguridad e la información y sistemas?
	¿Se cuenta con registro de eventos y pistas de auditoria que permitan la revisión de actividades de los usuarios, excepciones y fallos?
	¿Cuenta con controles que protejan de cambios no autorizados en dispositivos e información de registro o auditoria?
	¿Cuenta con pistas de auditoria y registro de actividades a nivel de sistemas y bases de datos los cuales monitorear las actividades de usuarios con privilegios?
	¿Cuenta con controles de sincronización de los relojes de los servidores desde una única fuente de tiempo precisa y acordada?
	¿ se cuenta con procedimientos para la actualización e instalación de software o cambios en producción?

	¿Cuentan con procedimientos que permitan identificar y gestionar la vulnerabilidades de los activos ?
	¿Cuenta con controles que permitan restringir y administrar la instalación de software?
	¿Existen procedimiento para un debido procesos de auditoria de sistemas operativos y organizacionales?
Seguridad en las Telecomunicaciones	¿Cuenta con controles de acceso a la red y servicios conectados frente a accesos no autorizados?
	¿cuenta con mecanismos de seguridad, niveles de servicio, y los requisitos de gestión para los servicios de red tanto internos como contratados?
	¿ Los servicios de información, los usuarios y los sistemas de información se encuentra segregados en distintas redes?
	¿Cuentan con políticas, procedimientos y controles formales que protejan el intercambio de información mediante canales de comunicación?
	¿se cuenta con acuerdos formales para el intercambio de información confidencial ente áreas organizaciones o terceros?
	¿Se cuenta con los controles para garantizar la seguridad en la mensajería electrónica?
	¿Cuentan con acuerdos de confidencialidad y no revelación de Información sensible?
Adquisición, desarrollo y Mantenimiento de los sistemas de información	¿se incluyen requisito de seguridad de la información en los requisitos de desarrollo de nuevos sistemas o mejoras de sistemas de información?
	¿Cuenta con controles de seguridad de la información para Las aplicaciones accesibles a través de redes públicas?
	¿cuenta con medidas de protección garanticen la confidencialidad, la integridad y el origen de los datos en las transacciones por redes telemáticas?
	¿Usan normas de desarrollo seguro en nuevos desarrollos o actualizaciones de los sistemas informáticos?
	¿Cuenta con procedimientos formales de control de cambios en el software?

	¿Realizan revisiones técnicas de las aplicación luego de realizar cambios o actualizaciones del sistema operativo?
	¿Maneja restricciones para el cambio en paquetes de software?
	¿Se hace uso de principios de ingeniería en protección de sistema para cualquier labor de implementación en los sistemas de información?
	¿Cuenta con procedimientos de desarrollo seguro?
	¿Cuenta con procedimientos para la supervisión y control del desarrollo de software externalizado?
	¿Realizan pruebas funcionales de seguridad durante el desarrollos de los sistemas?
	¿Usan enmascaramiento de datos u otros controles se seguridad para la información de los datos de pruebas?
Relaciones con Suministradores	¿Cuenta con políticas y acuerdos que permitan garantizar la seguridad de la información con los suministradores?
	¿Cuenta con acuerdos de gestión de riegos de la cadena de suministros con lo suministradores de TIC?
	¿Se realiza una supervisión y revisión con el fin de detectar posibles vulnerabilidades de los servicios prestados por terceros?
	Cuenta con acuerdos para la gestión de cambios en los servicios prestados por terceros?
Gestión de Incidentes	¿Cuneta con la gestión de responsabilidades y procedimientos para da respuesta rápida, efectiva y adecuada ate incidentes de seguridad e la información ?
	¿Cuenta con procedimientos para la notificación de incidentes o brechas de seguridad, puntos débiles identificados?
	¿Cuenta con procedimientos para la valoración de eventos de seguridad y toma de decisiones?
	¿Cuenta con procedimiento documentados para dar respuesta a incidente sede seguridad de la información?

	¿Cuenta con procedimientos para generar conocimiento a partir del análisis y la resolución de incidentes de seguridad de información con el fin reducir la probabilidad o impacto de incidentes futuros?
	¿Cuenta con procedimientos para la recopilación y preservación de información que pueda servir como evidencia en un incidente de seguridad e la información ?
Aspectos de la seguridad de la información en la Gestión de la Continuidad de Negocio	¿Cuenta con planes de Respuesta a Incidentes y Continuidad del Negocio, Recuperación de Incidentes y Recuperación de Desastres?
	¿Cuenta con procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa?
	¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad del negocio?
	¿Cuenta con redundancia de los recursos de tratamiento de la información?
Cumplimiento	¿Tiene documentado los requisitos legales, regulatorios y contractuales aplícales para la Unidad de sistematización Institucional?
	¿Cuenta con procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual?
	¿Cuenta con controles que permitan proteger los registros organizacionales para cumplir con los requisitos legales, reglamentarios o contractuales o soportar las actividades esenciales del negocio
	¿Cuenta con política de privacidad y protección de la información de carácter personal?
	¿cuenta con procedimientos para el uso de controles criptográficos basados en contratos, leyes y regulaciones pertinentes?

	¿cuenta con procedimientos para auditoria interna o externa de los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información?
	¿cuenta con procedimientos para la revisión y monitoreo del cumplimiento de las políticas y normas de seguridad?
	¿Se realizan periódicamente pruebas de intrusión y evaluación de vulnerabilidades de los sistemas?

_____

Firma del entrevistado

Nombre del entrevistado

ANEXO 2

MAPEO ISO 27002:2013 a CFS de NIST

ISO 27002:2013			CSF NIST		
DOMINIOS	**OBJETIVOS CONTROL**	**CONTROL**	**FUNCIÓN**	**CATEGORÍA**	**SUBCATEGORÍA**
5. Políticas de seguridad	5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información	**Identificar ID**	Gobernanza ID.GV	ID.GV-1: Se establece y se comunica la política de seguridad cibernética organizacional.
				Gobernanza ID.GV	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos..
		5.1.2 Revisión de las políticas para la seguridad de la información			
6. Aspectos Organizativos Seguridad de la Información	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la Seguridad de la Información	**Identificar ID**	Gestión de activos ID.AM	ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios están establecidas.
			Proteger PR	Concienciación y capacitación PR.AT	PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades

					PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
					PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.
					PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
			Detectar DE	Procesos de Detección DE.DP	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurarla responsabilidad.
			Responder RS	Comunicaciones RS.CO	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
		6.1.2 Segregación de tareas	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
			Responder RS	Comunicaciones RS.CO	RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.

		6.1.3 Contacto con las autoridades	**Responder RS**	Comunicaciones RS.CO	RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.
		6.1.4 Contacto con grupos de interés especial	**Identificar ID**	Evaluación de riesgos ID.RA	ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.
			Responder RS	Comunicaciones RS.CO	RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.
			Recuperar RC	Comunicaciones RC.CO	RC.CO-1: Se gestionan las relaciones públicas.
		6.1.5 Seguridad de la información en la gestión de proyectos	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
	6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-3: Se gestiona el acceso remoto.

		6.2.2 Teletrabajo	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-3: Se gestiona el acceso remoto.
7. Seguridad Ligada a los recursos humanos	7.1 Antes de la contratación	7.1.1 Investigación de antecedentes	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
		7.1.2 Términos y condiciones de contratación	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)

	7.2 Durante la contratación	7.2.1 Responsabilidades de gestión	**Identificar ID**	Gobernanza ID.GV	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos..
			Proteger PR	Concienciación y capacitación PR.AT	PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
		7.2.2 Concienciación, educación y capacitación en Seguridad de la Información	**Proteger PR**	Concienciación y capacitación PR.AT	PR.AT-1: Todos los usuarios están informados y capacitados.
					PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades
					PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.
					PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.

					PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
			Detectar DE	Procesos de Detección DE.DP	DE.DP-1: Los roles y los deberes de detección están bien definidos para asegurarla responsabilidad.
			Responder RS	Comunicaciones RS.CO	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
		7.2.3 Proceso disciplinario	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.

			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)
8. Gestión Activos	8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos	**Identificar ID**	Gestión de activos ID.AM	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados. ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariada
		8.1.2 Propiedad de los activos	**Identificar ID**	Gestión de activos ID.AM	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados. ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariada
		8.1.3 Uso aceptable de los activos			
		8.1.4 Devolución de activos	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal)

	8.2 Clasificación de la información	8.2.1 Directrices de clasificación	**Identificar ID**	Gestión de activos ID.AM	ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.
			Proteger PR	Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
		8.2.2 Etiquetado y manipulado de la información	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
				Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
		8.2.3 Manipulación de activos	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-1: Los datos en reposo están protegidos.
					PR.DS-2: Los datos en tránsito están protegidos.
					PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.

				Procesos y procedimientos de protección de la información PR.IP	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
				Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
	8.3 Manejo de los soportes de almacenamiento	8.3.1 Gestión de soportes extraíbles	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
				Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
		8.3.2 Eliminación de soportes	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.

				Procesos y procedimientos de protección de la información PR.IP	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
		8.3.3 Soportes físicos en tránsito	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
				Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
9. Control de Accesos	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		9.1.2 Control de acceso a las redes y servicios asociados	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.

				Tecnología de protección PR.PT	PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
					PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.
			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).

		9.2.2 Gestión de los derechos de acceso asignados a usuarios	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
		9.2.3 Gestión de los derechos de acceso con privilegios especiales	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
					PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		9.2.4 Gestión de información confidencial de autenticación de usuarios	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

					PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
		9.2.5 Revisión de los derechos de acceso de los usuarios			
		9.2.6 Retirada o adaptación de los derechos de acceso	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
	9.3 Responsabilidades del usuario	9.3.1 Uso de información confidencial para la autenticación	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

					PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
	9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		9.4.2 Procedimientos seguros de inicio de sesión	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

					PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
		9.4.3 Gestión de contraseñas de usuario	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.
					PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).

		9.4.4 Uso de herramientas de administración de sistemas	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		9.4.5 Control de acceso al código fuente de los programas	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
			Proteger PR	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
10. Cifrado	10.1 Controles criptográficos	10.1.1 Política de uso de los controles criptográficos	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		10.1.2 Gestión de claves:			
11. Seguridad física y Ambiental	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.

			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.
		11.1.2 Controles físicos de entrada	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Mantenimiento PR.MA	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.
		11.1.3 Seguridad de oficinas, despachos y recursos	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.

		11.1.4 Protección contra las amenazas externas y ambientales	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		11.1.5 El trabajo en áreas seguras	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		11.1.6 Áreas de acceso público, carga y descarga	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.

	11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.
		11.2.2 Instalaciones de suministro	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.
		11.2.3 Seguridad del cableado	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos

			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.
		11.2.4 Mantenimiento de los equipos	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.
				Mantenimiento PR.MA	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas
					PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.

		11.2.5 Salida de activos fuera de las dependencias de la empresa	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Seguridad de los datos PR.DS	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
				Mantenimiento PR.MA	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas
		11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	**Identificar ID**	Gestión de activos ID.AM	ID.AM-4: Los sistemas de información externos están catalogados
			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-3: Se gestiona el acceso remoto.

				Mantenimiento PR.MA	PR.MA-1: El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas
		11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.
				Seguridad de los datos PR.DS	PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-6: Los datos son eliminados de acuerdo con las políticas.
		11.2.8 Equipo informático de usuario desatendido	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-2: Se gestiona y se protege el acceso físico a los activos.

		11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.
12. Seguridad en la Operativa	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación	**Detectar DE**	Anomalías y Eventos DE.AE	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
		12.1.2 Gestión de cambios	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
			Detectar DE	Anomalías y Eventos DE.AE	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.

		12.1.3 Gestión de capacidades	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos
			Proteger PR	Seguridad de los datos PR.DS	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad
		12.1.4 Separación de entornos de desarrollo, prueba y producción	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.
	12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso	**Proteger PR**	Concienciación y capacitación PR.AT	PR.AT-1: Todos los usuarios están informados y capacitados.
				Seguridad de los datos PR.DS	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-4: Se detecta el código malicioso.
			Responder RS	Mitigación RS.MI	RS.MI-1: Los incidentes son contenidos.
				Mitigación RS.MI	RS.MI-2: Los incidentes son mitigados.

	12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.
	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
			Detectar DE	Anomalías y Eventos DE.AE	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
					DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.
				Monitoreo Continuo de la Seguridad DE.CM	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
					DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
			Responder RS	Análisis RS.AN	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.

		12.4.2 Protección de los registros de información	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
		12.4.3 Registros de actividad del administrador y operador del sistema	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.
			Responder RS	Análisis RS.AN	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.
		12.4.4 Sincronización de relojes	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.

	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-5: Se detecta el código móvil no autorizado.
	12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas	**Identificar ID**	Evaluación de riesgos ID.RA	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.

					ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-8: Se realizan escaneos de vulnerabilidades.
			Responder RS	Mitigación RS.MI	RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.
		12.6.2 Restricciones en la instalación de software	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-5: Se detecta el código móvil no autorizado.
	12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información	**Proteger PR**	Tecnología de protección PR.PT	PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.
13. Seguridad en las Telecomunicaciones	13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-3: Se gestiona el acceso remoto.
					PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red)
				Seguridad de los datos PR.DS	PR.DS-2: Los datos en tránsito están protegidos.
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
				Tecnología de protección PR.PT	PR.PT-4: Las redes de comunicaciones y control están protegidas.

			Detectar DE	Anomalías y Eventos DE.AE	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
		13.1.2 Mecanismos de seguridad asociados a servicios en red	**Detectar DE**	Anomalías y Eventos DE.AE	DE.AE-1: Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
		13.1.3 Segregación de redes	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red)
				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
	13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información	**Identificar ID**	Gestión de activos ID.AM	ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados
			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-3: Se gestiona el acceso remoto.
					PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red)
					PR.DS-2: Los datos en tránsito están protegidos.

				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
				Tecnología de protección PR.PT	PR.PT-4: Las redes de comunicaciones y control están protegidas.
		13.2.2 Acuerdos de intercambio	**Identificar ID**	Gestión de activos ID.AM	ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados
		13.2.3 Mensajería electrónica	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-2: Los datos en tránsito están protegidos.
					PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
		13.2.4 Acuerdos de confidencialidad y secreto	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
14. Adquisición, desarrollo y Mantenimiento de los sistemas de información	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
		14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red)
					PR.DS-2: Los datos en tránsito están protegidos.

				Seguridad de los datos PR.DS	PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
					PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
		14.1.3 Protección de las transacciones por redes telemáticas	**Proteger PR**	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red)
				Seguridad de los datos PR.DS	PR.DS-2: Los datos en tránsito están protegidos.
					PR.DS-5: Se implementan protecciones contra las filtraciones de datos.
					PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
				Tecnología de protección PR.PT	PR.PT-4: Las redes de comunicaciones y control están protegidas.

	14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro de software	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
		14.2.2 Procedimientos de control de cambios en los sistemas	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
		14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).

					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
		14.2.4 Restricciones a los cambios en los paquetes de software	**Proteger PR**	Seguridad de los datos PR.DS	PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-1: Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).
					PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.

		14.2.5 Uso de principios de ingeniería en protección de sistemas	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.
		14.2.6 Seguridad en entornos de desarrollo			
		14.2.7 Externalización del desarrollo de software	**Detectar DE**	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.
					DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
		14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	**Detectar DE**	Procesos de Detección DE.DP	DE.DP-3: Se prueban los procesos de detección.
		14.2.9 Pruebas de aceptación			
	14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en prueba			

15. Relaciones con Suministradores	15.1 Seguridad de la información en las relaciones con suministradores	15.1.1 Política de seguridad de la información para suministradores	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.
				Gobernanza ID.GV	ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos..
				Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
					ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.

			Proteger PR	Mantenimiento PR.MA	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.
		15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.
				Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
					ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.

		15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.
				Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
					ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.

				Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
					ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.
					ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
			Proteger PR	Mantenimiento PR.MA	PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.

			Detectar DE	Monitoreo Continuo de la Seguridad DE.CM	DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.
					DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.
		15.2.2 Gestión de cambios en los servicios prestados por terceros	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-1: Se identifica y se comunica la función de la organización en la cadena de suministro.
				Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
					ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.

					ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
16. Gestión de Incidentes	16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
			Detectar DE	Anomalías y Eventos DE.AE	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
			Responder RS	Comunicaciones RS.CO	RS.CO-1: El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.
		16.1.2 Notificación de los eventos de seguridad de la información	**Detectar DE**	Procesos de Detección DE.DP	DE.DP-4: Se comunica la información de la detección de eventos
			Responder RS	Comunicaciones RS.CO	RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.

		16.1.3 Notificación de puntos débiles de la seguridad	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
			Detectar DE	Procesos de Detección DE.DP	DE.DP-4: Se comunica la información de la detección de eventos
		16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones	**Detectar DE**	Anomalías y Eventos DE.AE	DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
				Anomalías y Eventos DE.AE	DE.AE-4: Se determina el impacto de los eventos
				Anomalías y Eventos DE.AE	DE.AE-5: Se establecen umbrales de alerta de incidentes.
			Responder RS	Análisis RS.AN	RS.AN-2: Se comprende el impacto del incidente.
					RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.
		16.1.5 Respuesta a los incidentes de seguridad	**Responder RS**	Planificación de la Respuesta RS.RP	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente
				Análisis RS.AN	RS.AN-1: Se investigan las notificaciones de los sistemas de detección.
				Mitigación RS.MI	RS.MI-1: Los incidentes son contenidos.

					RS.MI-2: Los incidentes son mitigados.
			Recuperar RC	Planificación de la recuperación RC.RP	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
		16.1.6 Aprendizaje de los incidentes de seguridad de la información	**Identificar ID**	Evaluación de riesgos ID.RA	ID.RA-4: Se identifican los impactos y las probabilidades del negocio.
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-7: Se mejoran los procesos de protección.
				Procesos y procedimientos de protección de la información PR.IP	PR.IP-8: Se comparte la efectividad de las tecnologías de protección.
			Detectar DE	Procesos de Detección DE.DP	DE.DP-5: los procesos de detección se mejoran continuamente.
			Responder RS	Análisis RS.AN	RS.AN-2: Se comprende el impacto del incidente.
				Mejoras RS.IM	RS.IM-1: Los planes de respuesta incorporan las lecciones aprendidas.
					RS.IM-2: Se actualizan las estrategias de respuesta

			Recuperar RC	Mejoras RC.IM	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
					RC.IM-2: Se actualizan las estrategias de recuperación.
		16.1.7 Recopilación de evidencias	**Detectar DE**	Anomalías y Eventos DE.AE	respuesta.
			Responder RS	Análisis RS.AN	RS.AN-3: Se realizan análisis forenses.
17. Aspectos de la Seguridad de la Información en la Gestión de la Continuidad de Negocio	17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).

		17.1.2 Implantación de la continuidad de la seguridad de la información	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.
					PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
				Tecnología de protección PR.PT	PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”) para lograr los requisitos de resiliencia en situaciones normales y adversas.

		17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**Identificar ID**	Gestión del riesgo de la cadena de suministro ID.SC	ID.SC-1: Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.
					PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
					PR.IP-10: Se prueban los planes de respuesta y recuperación
	17.2 Redundancias	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	**Identificar ID**	Entorno empresarial ID.BE	ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).

			Proteger PR	Seguridad de los datos PR.DS	PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad
			Proteger PR	Tecnología de protección PR.PT	PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o “hot swap”) para lograr los requisitos de resiliencia en situaciones normales y adversas.
18. Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales	18.1.1 Identificación de la legislación aplicable	**Identificar ID**	Gobernanza ID.GV	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
		18.1.2 Derechos de propiedad intelectual (DPI)	**Identificar ID**	Gobernanza ID.GV	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
		18.1.3 Protección de los registros de la organización	**Identificar ID**	Gobernanza ID.GV	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.

			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.
		18.1.4 Protección de datos y privacidad de la información personal	**Identificar ID**	Gobernanza ID.GV	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
			Proteger PR	Gestión de Identidad, autenticación y control de acceso PR.AC	PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
			Detectar DE	Procesos de Detección DE.DP	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables
		18.1.5 Regulación de los controles criptográficos	**Identificar ID**	Gobernanza ID.GV	ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
		18.2.1 Revisión independiente de la			

	18.2 Revisiones de la seguridad de la información	seguridad de la información			
		18.2.2 Cumplimiento de las políticas y normas de seguridad	**Proteger PR**	Procesos y procedimientos de protección de la información PR.IP	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
			Detectar DE	Procesos de Detección DE.DP	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables
		18.2.3 Comprobación del cumplimiento	**Identificar ID**	Evaluación de riesgos ID.RA	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.
			Proteger PR	Procesos y procedimientos de protección de la información PR.IP	PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.
			Detectar DE	Procesos de Detección DE.DP	DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables

ANEXO 3

DOMINIOS, OBJETIVOS Y CONTROLES DE LA NORMA ISO 27002: 2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.