UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
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
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Jorge Vinicio Gavidia Córdova
Tutor:
Christian Patricio Vaca Benalcázar

Quito – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Christian Patricio Vaca Benalcázar con C.I: 1719368555 en mi calidad de Tutor del proyecto de investigación titulado: 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.

Elaborado por: Jorge Vinicio Gavidia Córdova, de C.I: 1714852108, 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., 27 de septiembre de 2022

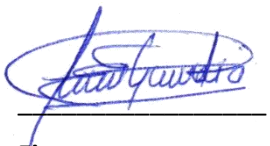
Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jorge Vinicio Gavidia Córdova con C.I: 1714852108, autor del proyecto de titulación denominado: 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. 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., 27 de septiembre de 2022



Firma

ORCID: 0000-0003-2248-2736

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

En la actualidad la tecnología ha tenido un crecimiento desmesurado, la automatización de procesos se ha convertido en una necesidad para la mayoría de instituciones que ofrecen servicios y más aún en instituciones dedicadas a la educación donde el manejo de la información es sensible y necesaria para cada una de las actividades diarias que necesitan hacer tanto docentes como estudiantes de una institución académica.

En el ámbito académico es importante contar con un proceso automatizado, que nos permita el ingreso de notas, toma de exámenes, generación de asistencia, y evaluaciones periódicas tanto a docentes como a estudiantes. El cual, al ser información con un nivel alto de confidencialidad e importancia, como por ejemplo los registros de notas y kardex académicos, se necesita poseer estrategias, métodos y técnicas de control de acceso para salvaguardar los datos que se manejan.

Actualmente la información representa uno de los activos más importantes de una institución, debido al crecimiento importante de ataques realizados en los últimos años es necesario contar con los controles adecuados para contrarrestar y minimizar los accesos no autorizados a los sistemas informáticos y de esta manera evitar la pérdida o robo de la información. (Castro, Figueroa, Vera, Álava, Parrales, Murillo, Castillo, 2018)

Con la presente investigación se establecen las diferentes metodologías para el análisis de vulnerabilidades de un sistema informático, aplicando los estándares adecuados para un mejor entendimiento del control de accesos y la importancia de contar con mecanismos de control que regulen el ingreso inapropiado a un sistema de gestión estratégica.

Garantizar los tres pilares fundamentales de la información que son la confidencialidad, integridad y disponibilidad son fundamentales en este mundo tecnológico, ahora también las instituciones educativas necesitan fortalecer los accesos y monitorear de manera constante alguna posible intrusión que pueda poner en riesgo la información.

Problema de investigación

Las instituciones de nivel superior o también conocidas por sus siglas (IES), son aquellas instituciones que proporcionan un servició público de educación y están reguladas por un organismo superior en nuestro país el Consejo de educación Superior (CES), que es el encargado de planificar, regular y coordinar el Sistema de Educación Superior.

De acuerdo a la información obtenida en CES en la actualidad el Ecuador cuenta con:

Tabla 1

Tipos de Instituciones a nivel nacional

Tipo de Institución	Número
Públicas nacionales	32
Públicas que operan en el Ecuador bajo acuerdos y convenios internacionales	2
Particulares que reciben asignaciones y rentas del Estado	8
Particulares autofinanciados	21

Nota: Elaboración propia

Las cuales se encuentran distribuidas a nivel nacional.

El entorno de desarrollo de los procesos en una institución de nivel superior se torna cada vez más complejo ya que el incremento de la tecnología obliga a buscar nuevos medios para el tratamiento de la información, toda institución necesita registrar, procesar, almacenar, recuperar y presentar información de manera rápida y confiable, de ahí la necesidad de contar con un sistema integrado que facilite el manejo de la información. La manera en que se gestione la educación superior desde las instancias gubernamentales y desde las propias IES será la diferencia entre el éxito y el fracaso. (Gallegos, 2022)

La Universidad Tecnológica Israel, maneja información muy importante de estudiantes, profesores y administrativos, toda esta información se maneja a través del Sistema Integrado de Gestión Estratégica (SIGE) un proyecto de investigación de la carrera de Sistemas de Información que nace en el año 2017 y se basa en procesos estratégicos y operativos. (Baldeón, 2022).

Al ser una herramienta muy utilizada en la actualidad por la comunidad de la UISRAEL, requiere una serie de controles que deben implementarse, para evitar posibles ataques o robo de información al acceder a la plataforma con el uso de credenciales poco seguras. Bajo esta premisa se puede plantear la siguiente pregunta:

¿Con los actuales controles de acceso que cuenta el Sistema Integrado de Gestión Estratégica SIGE alineados a un estándar internacional como la ISO 27002 y CSF de NIST mejorara la seguridad de la información de este aplicativo?

Objetivo general

Desarrollar un modelo de seguridad informática aplicando ISO 27002 y CSF de NITS, para mejorar el nivel de control de accesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, de acuerdo a los principios de calidad de Sistemas de Gestión de la Información.

Objetivos específicos

1. Contextualizar los fundamentos teóricos sobre las normas ISO 27002 y CSF de NIST en el dominio de control de accesos, con respecto a seguridad informática aplicada a sistemas de gestión estratégica.
2. Analizar la situación actual sobre control de accesos de acuerdo a la ISO 27002 y CSF de NIST del Sistema Integrado de Gestión Estratégica de la Universidad Israel.
3. Diseñar un modelo para control de accesos en seguridad informática aplicando ISO 27002 y CSF de NITS, del Sistema Integrado de Gestión Estratégica de la Universidad Israel.

Vinculación con la sociedad y beneficiarios directos:

Este trabajo está dirigido al personal del área de sistematización de la Universidad tecnológica Israel que son los encargados del desarrollo de la aplicación y son los responsables del buen funcionamiento del sistema. Las normas utilizadas para la investigación ayudarán a la toma de decisiones con respecto al control de accesos y puede tomarse como ejemplo para otras instituciones que también hagan uso de algún sistema integrado de gestión estratégica.

Este trabajo tiene como objetivo buscar las mejores políticas de seguridad que beneficiarán directamente la comunidad de la Universidad Israel garantizando un buen funcionamiento del SIGE y asegurando la protección de los datos que se almacenan diariamente gracias a la búsqueda de vulnerabilidades en el control de accesos, garantizando un manejo óptimo de la información y proporcionando servicios de calidad.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Con el avance de la tecnología en los últimos años, la información está cada vez más cerca de las personas, tan solo con unos cuantos clics se puede acceder a información existente en la red. De la misma manera que la tecnología avanza, los ataques informáticos también se hacen cada vez más sofisticados y se usan diferentes métodos o técnicas para engañar a las personas, algunas con el propósito de obtener contraseñas para el acceso a información confidencial de alguna institución, por ello es importante contar con una serie de controles que garanticen la seguridad de la información.

> De acuerdo a lo mencionado por Álvarez y Andrade (2020), "la seguridad de la información consiste en implementar planes y estrategias en el manejo de procesos, siendo la información considerada como un activo principal". Este conjunto de estrategias parte del establecer controles, políticas y procedimientos, cuyo objetivo principal es la detección de amenazas o vulnerabilidades que pongan en riesgo los activos de una institución y de esta manera proteger y garantizar el uso de la información.

Cabe destacar que las instituciones financieras, públicas o de salud no son las únicas que presentan algún riesgo de recibir algún ataque, las instituciones educativas también pueden ser víctimas de los ciber delincuentes. Los últimos acontecimientos sucedidos con motivo de la pandemia llevaron a las personas a realizar intercambios de información de forma descontrolada, con accesos a sistemas en grandes cantidades, sin contar con controles adecuados y sin la capacitación necesaria, por lo que hace vulnerable la información que se maneja dentro de una institución si no se establecen los controles adecuados, como marcos de trabajo o estándares internacionales (Guerra, 2021)

Según Sánchez (2021), define un marco de trabajo de seguridad como "un conjunto de estándares, normas o buenas prácticas que permiten controlar los riesgos que las tecnologías digitales presentan". Principalmente implementa una serie de objetivos concretos de seguridad los cuales ayudarán a controlar el acceso no autorizado y uso adecuado en la utilización de usuarios y contraseñas.

Existen varios estándares de seguridad de la información entre los cuales se mencionan los siguientes:

- Los estándares ofrecidos por la familia de la ISO 27000, es un estándar compuesto de varias normas de seguridad de la información, que nos indican las pautas para el desarrollo de un sistema de gestión de la información. En la tabla 2 se menciona el conjunto de normas que se encuentran dentro de esta familia, las cuales se describen a continuación:

Tabla 2

Conjunto de normas de la familia ISO 27000

Norma	Descripción
ISO/IEC 27000	Es el estándar SGSI principal de la cual se derivan todas las normas existentes.
ISO/IEC 27001	Es un estándar internacional para la gestión de la seguridad de una institución, es considerada como la norma más importante de la familia ya que promueve la mejora continua de cada uno de los procesos. Es un estándar internacional publicado en octubre de 2005.
ISO/IEC 27002	Aparece el 1 de julio de 2007, el objetivo principal es establecer diferentes recomendaciones para preservar la integridad, confidencialidad y disponibilidad de la información.
ISO/IEC 27003	Es un estándar internacional que nace como una guía para la implementación de un SGSI, fue publicada el 7 de diciembre del 2009 como soporte a la norma ISO 27001.
ISO/IEC 27004	Es un estándar que proporciona métricas de la gestión de la información. Identifica quien, como y cuando realizar medidas a los parámetros establecidos. Fue Publicada el 7 de diciembre del 2009.
ISO/IEC 27005	Es un estándar dedicado a la gestión de riesgos. Establece una serie de recomendaciones para evaluar la seguridad de la información. Es un soporte en los riesgos de la norma ISO 27001. Fue Publicada en junio de 2008.
ISO/IEC 27006	Proporciona los requisitos de acreditación para una organización. Se encarga de suministrar los requisitos y las guías para la certificación de un SGSI, es una auditoría para el cumplimiento de la norma ISO 27001. Nace en el año 2011.
ISO/IEC 27007	Constituye una guía para organizaciones certificadas, es una orientación para gestionar una auditoría a un SGSI.
ISO/IEC 27799:2008	Es un estándar basado en normas para la industria de la salud.

Nota: Tomado de Familia de Normas ISO 27000

- Estándares de la familia NIST: es un estándar que ayuda a las empresas a gestionar los riesgos, protege sus datos mediante el uso de un lenguaje común de correspondiente a prácticas de seguridad de la información (Villamizar, 2022)
- Controles de Servicio y Organización 2 (SOC 2): Consiste en el desarrollo de informes que se desarrollan sobre los controles que una organización debe tener para proteger la información. (Martín, 2021).
- SANS: es una institución con fines de lucro que agrupa a una serie de profesionales de seguridad informática, se basa principalmente en detectar vulnerabilidades en el desarrollo de software.
- ENS y serie 800 del CNN-CERT, Modelos COSO y COBIT entre otras.

1.2. Proceso investigativo metodológico

Investigación Bibliográfica

La investigación bibliográfica se la puede definir como una revisión de todo el material existente y disponible relacionado con el tema de investigación, el mismo que permitirá seleccionar la información relevante acorde a las fuentes de información utilizadas las cuales pueden estar contenidas en libros, revistas, videos entre otras. Se considera un paso fundamental, ya que implica una serie de puntos en base a la observación, investigación, interpretación, reflexión y análisis con el fin de obtener los fundamentos necesarios para el desarrollo de la investigación. (lifeder, 2020).

El proceso de investigación utilizado para este trabajo es bibliográfico exploratorio, porque se revisaron varias fuentes de autores, entre libros, artículos, revistas con el fin de obtener una visión general del problema existente en el control de accesos. Y cualitativa porque se realiza una propuesta de controles de seguridad para ser aplicadas dentro de una institución.

La investigación cualitativa

QuestionPro (2022) menciona que “es un proceso investigativo que permite conocer a fondo el tema. Provee información importante sobre un tema específico a través del estudio del comportamiento, las emociones y otros aspectos de la psicología humana que están abiertos a la interpretación”.

Tipo de investigación – Descriptiva

Se utiliza un tipo de investigación descriptiva que permite determinar el estado actual del control de accesos en una institución de nivel superior, conjuntamente con la etapa de la revisión analítica de la literatura.

Según Guevara (2020), "El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas".

El desarrollo de esta investigación se evalúa directamente en el área de Sistematización que es la encargada del soporte e implementación del Sistema Integrado de Gestión Estratégica dentro de la cual se podrá determinar cuál es el manejo con el que actualmente se realizan los procesos y se logrará determinar las posibles vulnerabilidades en el control de accesos que presente el sistema y que puedan poner en riesgo la información.

Técnicas e instrumentos de investigación.

Para el desarrollo de esta investigación se utiliza la entrevista, la cual proporcionará la información necesaria para complementar el estudio, sobre la situación actual del control de accesos en el sistema integrado de gestión estratégica (SIGE) de la Universidad Tecnológica Israel.

Entrevista: Es una comunicación establecida entre un investigador y la persona que va a servir como sujeto de estudio, con el fin de obtener respuestas en base al problema planteado las cuales ayudaran a resolver las interrogantes correspondientes al tema de estudio. (Tesis y Masters, 2021)

Población y muestra

De acuerdo al proceso investigativo metodológico del presente trabajo, se tiene una población a la Unidad de Sistematización Institucional (SI) de la Universidad Tecnológica Israel; y con una muestra, de dos profesionales responsables del desarrollo e implementación del SIGE. Es un tipo de muestra intencionada por las responsabilidades que poseen los profesionales de la SI.

1.3. Análisis de resultados

Para determinar la vulnerabilidad existente se realiza una comparativa entre la ISO 27002:2013 y CSF de NIST versus lo aplicado en el Sistema Integrado de Gestión Estratégica (SIGE).

De la comparativa realizada se puede determinar qué porcentaje de controles se encuentran implementados en la actualidad y cuales son necesarios para su implementación.

Una vez realizada la comparativa entre los dos estándares internacionales, se puede determinar cuáles son las vulnerabilidades que actualmente se presentan, para ello se realiza una entrevista al director del área de Sistematización y el jefe de programadores que gracias a su experticia proporcionan información importante para diagnosticar el estado actual del sistema.

Para el desarrollo de esta investigación se logró recopilar información importante con la cual se logra sustentar el objeto de estudio, los orígenes de las fuentes obtenidas son confiables y garantizan un buen desenvolvimiento en el tema planteado.

Investigaciones previas realizadas

Existen varios estudios realizados, basados en el control de accesos en universidades, se ha seleccionado los que van más acordes a nuestra investigación y se detallan a continuación:

En la investigación realizada por Morales (2021) se menciona que:

> Una Institución educativa de nivel Superior necesita incentivar la creación, desarrollo, transmisión y sobre todo promover la difusión de la ciencia, la técnica, la tecnología y la cultura en base al uso de las distintas herramientas tecnológicas existentes.
>
> En el Ecuador todavía no se ha llevado a cabo una estrategia con respecto a la ciberseguridad que contengan lineamientos necesarios para proteger la información, la infraestructura y en especial a los usuarios frente a algún ataque.

Según la investigación realizada por Chávez (2018) se menciona que:

> Las normas ISO 27001 – 27002 gestionan la seguridad de la información
>
> En una Institución de Educación Superior es muy importante preservar la confidencialidad, integridad y disponibilidad de la información.
>
> El uso normativo citado en base a las normas ISO, es necesario para afianzar la seguridad de una base de datos, por lo que, la confidencialidad, integridad y disponibilidad de la información pueden ser garantizadas en los cada uno de los procesos.

Según la investigación realizada por Cueva (2015) se menciona:

> Desarrollar un plan de gestión de riesgos de TI con la metodología NIST SP 800-30 brinda la oportunidad de comprender conceptos relacionados con la gestión de riesgos.

> Con el aumento de la tecnología, también aumenta el riesgo existente ante algún posible ataque tanto para instituciones públicas o privadas de manera que afectan las actividades diarias de la organización y causaran pérdidas significativas por tanto es importante controlar las posibles vulnerabilidades a las que se encuentran expuestas las organizaciones.

En la investigación realizada por MOLINA (2020) se menciona:

> Que el uso del estándar proporcionado por NIST ayuda a identificar los activos, amenazas y vulnerabilidades de la información.
>
> El Instituto Nacional de Estándares y Tecnología tiene controles de infraestructura estricta que aborda la identificación, evaluación y gestión del riesgo cibernético a través de acciones flexibles, necesarias y constantes basadas en el desempeño y la rentabilidad, incluida la identificación y el desarrollo de un marco de riesgo de seguridad cibernética.

De estos estudios realizados se puede determinar que el uso de estos estándares, representa un avance significativo para una institución si se la implementa de manera óptima y así poder contrarrestar las amenazas que diariamente aquejan a un sistema informático.

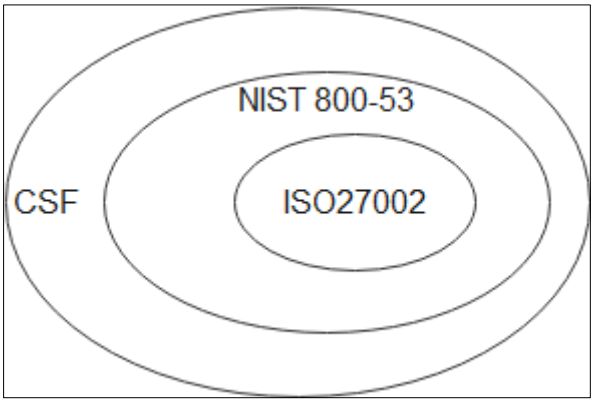
CAPÍTULO II: PROPUESTA

1.1. Fundamentos teóricos aplicados

En esta investigación se utilizan el estándar ISO 27002: 2013 y CSF de NIST debido a que, la primera establece directrices importantes para mantener, implementar o mejorar la seguridad de la información y la segunda es un súper conjunto de la primera como se puede evidenciar en la Figura 1, es decir ayuda a reforzar la seguridad en caso de que la ISO 27002:2013 no cubra todo el rango necesario.

Figura 1

Estructura de controles dentro de CSF



Nota: elaboración propia

El objetivo principal de la norma ISO 27002 es proporcionar un control en el acceso con el uso de un sistema de normas, restricciones y procedimientos que garanticen la asignación de derechos de acceso a cada uno de los sistemas de información. (ISOTools Excellence, 2017).

Se elige la versión ISO 27002:2013 debido a su tiempo de aplicación es decir es más probada que la ISO27002:2022, si bien es cierto la 2022 aborda aspectos más actuales como ciberseguridad y temas relacionados con la protección de datos y privacidad es un marco reciente mente publicado lo que la convierte en menos probada. A continuación, en la tabla 3, se detallan algunas de las diferencias existentes entre la versión 2013 y 2022:

Tabla 3

Diferencias entre ISO 27002:2013 y 27002:2022

ISO/IEC 27002:2013	ISO/IEC FDIS 27002:2022
Tecnología de la información – técnicas de seguridad – código de práctica para	Seguridad de la información, ciberseguridad y protección de la privacidad- controles de seguridad de la información

controles de seguridad de la información	
114 controles	93 controles
14 categorías	4 categorías y 2 anexos

Nota: tomado de HKMEXICO (2022)

En la tabla 4 se realiza un análisis comparativo de los controles de la norma ISO en sus dos versiones, donde se puede identificar el número de controles por dominio y se detallan a continuación:

Tabla 4

Controles utilizados por los estándares en sus dos versiones

ISO/IEC 27002:2013		**ISO/IEC FDIS 27002:2022**	
Políticas de seguridad de la información	2	Controles Organizacionales	37
Organización de seguridad de la información	7	Controles de Personas	8
Seguridad en recursos humanos	6	Controles Físicos	14
Gestión de Evaluación	10	Controles Tecnológicos	34
Control de Acceso	14		
Criptografía	2		
Seguridad física y ambiental	15		
Seguridad de operaciones	14		
Seguridad en las comunicaciones	7		
Adquisición, desarrollo y mantenimiento de sistema	13		
Relaciones con proveedores	5		
Gestión de incidentes de seguridad de la información	7		
Aspectos de seguridad de la información y continuidad de negocio	4		

Nota: cuadro que muestra los controles de la ISO 27002 en sus dos versiones, tomado de HKMEXICO (2022)

Una vez establecidos los estándares a utilizar, es necesario conocer un poco más sobre cada uno de ellos y establecer el dominio que servirá como base de esta investigación.

National Institute of Standards and Technology (NIST)

El Cyber Security Framework (CSF) de NIST o marco de seguridad cibernético, es un marco para la mejora de la seguridad de la información, fue desarrollada en los Estados Unidos en el año 2013 y actualmente se encuentra en la versión 1.1 que fue liberada en al año 2018. (Almagro, 2019, p. 3)

El la figura 2 se muestran los 5 marcos de referencia incluidos en el Framework:

Figura 2
Funciones del CSF

Nota: Almagro (2019)

Estas cinco funciones representan los pilares para un programa de seguridad exitoso. En la tabla 5 se menciona de forma detallada cada uno de los mismos:

Tabla 5

Funciones del CSF NIST

Funciones	Descripción
Identificación	Permite identificar los riesgos, las personas, los activos, los datos y las capacidades de una organización
Protección	Controla quienes acceden a la red, utiliza medios de encriptación de la información mientras leen o almacenan datos para evitar filtraciones
Detección	Monitoreo constante del servidor de aplicación para detectar posibles accesos no autorizados
Respuesta	Notificaciones oportunas, a los usuarios en caso de algún riesgo, mantener activas todas las operaciones de la institución, aplicar las mejores técnicas para contrarrestar algún ataque
Recuperación	Notificaciones oportunas, a los usuarios en caso de algún riesgo, mantener activas todas las operaciones de la institución, aplicar las mejores técnicas para contrarrestar algún ataque

Nota: Elaboración propia

NIST 800-53 aborda aspectos de la ISO 27002 por lo tanto, le convierte en un super conjunto de controles y aporta nuevos controles cubriendo un rango más amplio, su objetivo principal es estandarizar las buenas prácticas que garanticen la protección de los activos informáticos (complianceforge.com, 2020).

En el anexo 3 se muestra una tabla de controles establecidos por el estándar NIST versus los controles establecidos por ISO27001, a partir de estos controles establecidos por las dos normas se extraen los controles necesarios para esta investigación la cual se basa en el control de accesos.

ISO 27002:2013

El estándar internacional ISO 27002:2013 está orientado a la seguridad de la información de cualquier organización, de modo que al sufrir alguna amenaza se minimice al máximo la pérdida o robo de la información. Este estándar está conformado por los siguientes controles:

- Política de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Cifrado
- Seguridad en la operativa
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Relaciones con suministradores
- Cumplimiento. (iso27000.es, 2013).

El presente estudio se basa en el dominio de control de accesos. Todo acceso no autorizado debe ser controlado y debe minimizarse la probabilidad de que esto suceda, se debe identificar de manera adecuada el rol que debe tener cada usuario, para de esta manera tener un control adecuado al acceso de la información. A continuación, se detallan los controles que hace mención este dominio en base a los establecido por el estándar ISO27002:2013:

- **Requisitos de negocio para el control de accesos**

  Consiste en controlar el acceso solo a personal autorizado, el mismo se divide en los siguientes controles:

  Política de control de acceso: Consiste en un conjunto de reglas que controlan el acceso a la información, en este control son los propietarios quienes definen que normas se deben aplicar.

  Control de acceso a las redes y servicios asociados: Consiste en autorizar a los usuarios para que tengan acceso a las redes y servicios de red.

- **Gestión de acceso de usuario**

  Es necesario establecer una serie de procesos que permitan controlar la asignación de usuarios y los permisos que debe tener cada uno, desde el momento que se registra en el sistema, hasta que sea dado de baja, de esta manera se puede cubrir el ciclo de vida de acceso a un usuario de acuerdo a lo establecido por la norma ISO 27002.

  Garantiza el acceso a usuarios autorizados por medio de procesos establecidos, y evita el acceso a usuarios no autorizados. Dentro de la gestión de acceso de usuarios tenemos los siguientes controles:

  Gestión de altas y bajas en el registro de usuarios

  El área de seguridad será la encargada de asignar y dar de baja a los usuarios para el acceso al sistema. Siguiendo aspectos importantes como nombres de usuario únicos, asignación de roles pertinentes al área en que se desenvuelve.

  Gestión de los derechos de acceso asignados a usuarios

  Son herramientas que permiten la asignación y restricción de permisos a los sistemas de información.

  Gestión de los derechos de acceso con privilegios especiales

  Consiste en identificar a los usuarios que requieren de permisos especiales para el acceso y debe ser detallado por escrito.

  Gestión de información confidencial de autenticación de usuarios

  Consiste en la asignación de contraseñas a los usuarios previa autorización del jefe del departamento.

  Revisión de los derechos de acceso de los usuarios

  Consiste en realizar monitoreo o revisiones constantes sobre los permisos asignados a los usuarios.

  Retirada o adaptación de los derechos de acceso

  Consiste en realizar un bloqueo general de los accesos cuando un funcionario haya sido retirado de su cargo.

- **Responsabilidades del usuario.**

  El objetivo de este control es determinar las responsabilidades que tiene cada uno de los usuarios, cada usuario es responsable del rol asignado y debe ser consciente de la información que maneja

  Uso de información confidencial para la autenticación

  Es necesario que el usuario tenga claro el uso de buenas prácticas como el uso de contraseñas seguras y no divulgar sus accesos a otras personas.

- **Control de acceso a sistemas y aplicaciones**

  Es necesario establecer políticas de acceso que protejan la información ya sean documentos o cualquier otro medio informático para evitar accesos no autorizados.

  Restricción del acceso a la información

  Definir políticas de control que definan la restricción en el acceso a los sistemas de información.

  Procedimientos seguros de inicio de sesión

  Son controles para el inicio de sesión seguros, capaces de reconocer la identidad de una persona.

  Gestión de contraseñas de usuario

  Son sistemas capaces de generar contraseñas seguras, esto incluye la renovación continua de las mismas en tiempos determinados.

  Uso de herramientas de administración de sistemas

  Todo sistema con acceso privilegiado debe utilizar una autenticación por separado, es decir deben ser administrados de manera independiente para evitar que estas interfieran en el sistema.

  Control de acceso al código fuente de los programas.

  Es necesario aplicar restricciones al código fuente de la aplicación mediante el uso de librerías, el código debe ser administrado en un entorno fuera de la red principal.

1.2. Descripción de la propuesta

El análisis realizado para determinar las vulnerabilidades existentes en el SIGE se lo realiza mediante una comparativa entre los estándares internacionales ISO 27002:2013 y CSF de NIST en la que se describen los posibles controles que maneja cada una, además permite una

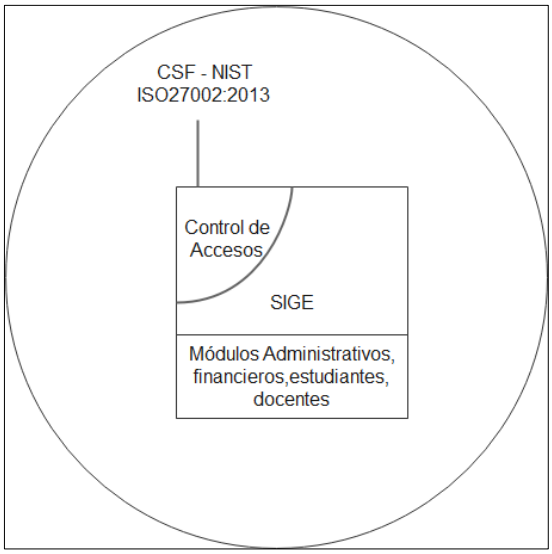
mayor comprensión de hacia dónde van orientadas y proporciona una base adecuada para el manejo de control de accesos.

a. Estructura general

A continuación, en la figura 3, se detalla la estructura actual que presenta el SIGE y como el control de accesos interviene en la parte de acceso a la información. De igual manera se representa gráficamente como los estándares internacionales deben cubrir esa puerta de enlace, para garantizar el acceso solo de personas autorizadas.

Figura 3

Estructura de aplicación de los estándares al control de accesos



Nota: Elaboración propia

En la tabla 6 se muestra un enfoque general de los dos estándares utilizados donde se determina de manera resumida la estructura de los controles con los que cuenta cada una.

Tabla 6

Enfoque en que se basa de NIST vs ISO 27002:2013

NIST	ISO 27002:2013
NIST se creó principalmente para ayudar a las agencias y organizaciones federales de EE. UU. A gestionar mejor su riesgo	ISO 27002:2013 es un enfoque reconocido internacionalmente para establecer y mantener un SGSI
Los marcos NIST tienen varios catálogos de control	ISO 27002:2013 proporciona 14 categorías de control con 114 controles
El marco NIST CSF contiene tres componentes clave: el núcleo, los niveles de implementación y los perfiles, y cada función tiene categorías, que son las actividades necesarias para cumplir con cada función.	ISO 27002:2013 es menos técnica, con más énfasis en la gestión basada en riesgos que brinda recomendaciones de mejores prácticas para asegurar toda la información

NIST tiene un mecanismo voluntario de auto certificación	ISO 27002:2013 se basa en organismos independientes de auditoría y certificación
El marco NIST utiliza cinco funciones para personalizar los controles de ciberseguridad	ISO 27002:2013 tiene diez cláusulas para guiar a las organizaciones a través de su SGSI

Nota: Tomado de itgovernance (2022)

b. Explicación del aporte

Una vez determinado el enfoque entre los dos estándares como lo muestra en la Tabla 7 y en base a la estructura de la Figura 3, se puede determinar el amplio rango de control que se aplican en una institución. Esta investigación se basa principalmente en el dominio de control de accesos para lo cual es necesario realizar una comparativa de lo que mencionan los dos estándares versus lo aplicado en la actualidad en el SIGE como se muestra a continuación:

Tabla 7

Tabla comparativa ISO 2002:2013 vs NIST SP 800-53

	NIST SP 800-53 CONTROLES	**ISO/IEC 27002:2013 CONTROLES** ***Nota: Un asterisco (*) indica que el control ISO/IEC no satisface plenamente la intención del control NIST.***	**Sistema Integrado de Gestión Estratégica (SIGE)**
AC-1	Política y procedimientos de control de acceso	A.9.1.1	Cumple
AC-2	Gestión de cuentas	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	Cumple
AC-3	Aplicación de acceso	A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5	Cumple
AC-6	Privilegio mínimo	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	
AC-7	Intentos de inicio de sesión fallidos	A.9.4.2	Cumple
AC-8	Notificación de uso del sistema	A.9.4.2	Cumple
AC-9	Notificación de inicio de sesión anterior	A.9.4.2	
AC-10	Control de sesión concurrente	Ninguno	
AC-24	Decisiones de control de acceso	A.9.4.1*	
CA-7	Monitoreo continuo	9.1, 9.2	

CA-8	Pruebas de penetración	Ninguno				
CA-9	Conexiones internas del sistema	Ninguno				
CM-5	Restricciones de acceso para el cambio de contraseñas	A.9.2.3				Cumple
CM-6	Configuración	Ninguno				
IA-2	Identificación y autenticación (usuarios de la organización)	A.9.2.1				Cumple
IA-4	Gestión de identificadores	A.9.2.1				
IA-5	Gestión de autenticadores	A.9.2.1, A.9.4.3	A.9.2.4,	A.9.3.1,		
IA-6	Comentarios sobre la autenticación	A.9.4.2				
IA-8	Identificación y autenticación (usuarios no organizacionales)	A.9.2.1				Cumple
IA-9	Identificación y autenticación de servicios	Ninguno				
IA-10	Identificación y autenticación adaptables	Ninguno				
IA-11	Re autenticación	Ninguno				
IA-12	Prueba de identidad	Ninguno				

Nota. NIST (2020).

De acuerdo a la tabla comparativa realizada se establecen los siguientes resultados en base a los siguientes criterios, los mismos serán utilizados tanto para la entrevista como para la observación y son los siguientes:

- Se agrupan por número de controles de acuerdo al control al que pertenecen.
- Se establece un porcentaje de ponderación en base a la importancia que tienen los controles, siendo los valores más altos los controles más importantes.
- De acuerdo al número de controles existentes en cada grupo se establece una regla de tres simple para determinar el porcentaje que se obtiene en la comparativa realizada.
- Se suman los porcentajes obtenidos en cada grupo para obtener el porcentaje total de controles aplicados, con los cuales podemos establecer cuáles son los riesgos que se presentan en el SIGE.

En la tabla 8 se pude observar los cálculos realizados en la tabla comparativa.

Tabla 8
Resultados tabla comparativa

Descripción	Siglas	Nro. Controles	Ponderación %	Resultado evaluación %
CONTROL DE ACCESO	AC	9	30%	20%
EVALUACIÓN Y AUTORIZACIÓN DE SEGURIDAD	CA	3	25%	0%
POLÍTICA Y PROCEDIMIENTOS DE GESTIÓN DE LA CONFIGURACIÓN	CM	2	15%	7.5%
POLÍTICA Y PROCEDIMIENTOS DE IDENTIFICACIÓN Y AUTENTICACIÓN	IA	9	30%	6.66%
Total		**23**		**30.83%**

Nota: Elaboración propia

c. Estrategias y técnicas utilizadas

Esta investigación se basa en conceptos previos realizados por otros investigadores, las cuales ayudan a elaborar un modelo de seguridad informática en el control de accesos, en base a los requerimientos establecidos por las normas seleccionadas.

Como base para la obtención de las vulnerabilidades se realiza una entrevista formada por los principales controles establecidos por la ISO 27002:2013 en el dominio de control de accesos y que están contenidos dentro de CSF de NIST tabla 9.

1.3. Validación de la propuesta

De la comparativa realizada en la Tabla 8, se puede determinar que únicamente se cumple con un porcentaje del 30.83% de controles utilizados. Este porcentaje se lo pudo obtener gracias a una observación realizada en el área de sistematización una vez firmada el acta de reserva confidencialidad proporcionada por el director del área. De la misma manera y aplicando la misma técnica de la observación se obtiene los porcentajes en base a los controles

proporcionados por el estándar internacional ISO27002:2013 que se encuentran aplicados en el SIGE, Tabla 9.

Tabla 9

Resultados observación realizada área de Sistematización.

Control de accesos ISO 27002	Preguntas (dominio 9 ISO 27002_2013)	Resultado
9.1 Requisitos de negocio para el control de acceso	1. ¿Cuenta con una política de control de acceso basada en los requisitos de negocio?	0
	2. ¿El acceso a las redes y servicios asociados lo realizan solo los usuarios autorizados?	1
9.2 Gestión de acceso de usuario	3. ¿Existe un proceso para gestión de altas/bajas en el registro de usuarios?	1
	4. ¿Cuenta con un procedimiento formal para gestión de los derechos de acceso asignados a usuarios?	1
	5. ¿Cuentan con un control en gestión de los derechos de acceso con privilegios especiales?	0
	6. ¿Cuentan con un proceso de gestión de información confidencial de autenticación de usuarios?	0
	7. ¿Realizan revisiones de los derechos de acceso de los usuarios?	0
	8. ¿Se realiza una retirada o adaptación de los derechos de acceso de forma adecuada cuando una persona finaliza sus actividades en la institución?	0
9.3 Responsabilidades del usuario	9. ¿Existe uso de información confidencial para la autenticación?	0
9.4 Control de acceso a sistemas y aplicaciones	10. ¿Existe alguna restricción del acceso a la información?	1
	11. ¿Existen procedimientos seguros de inicio de sesión?	1
	12. ¿Cuentan con un sistema de gestión de contraseñas de usuario?	1
	13. ¿Hacen uso de herramientas de administración de sistemas?	0

14. ¿Existe un control de acceso al código fuente de los programas?	0

Nota: Obtenido del Área de Sistematización (UISRAEL)

Como resultado del análisis realizado y con base a los resultados obtenidos en la observación podemos determinar que existen fallas en el control de accesos que deben ser tratadas a la brevedad, lo cual convierte al Sistema Integrado de Gestión Estratégica en vulnerable si no se controla adecuadamente.

En la tabla 10 se muestra como resultado de la evaluación los siguientes porcentajes obtenidos en base a la observación realizada aplicando el estándar de la norma ISO27002:2013, los mismos que servirán para comparar los resultados proporcionados por NIST en base a la entrevista y se muestran a continuación:

Tabla 10

Porcentaje de controles aplicados

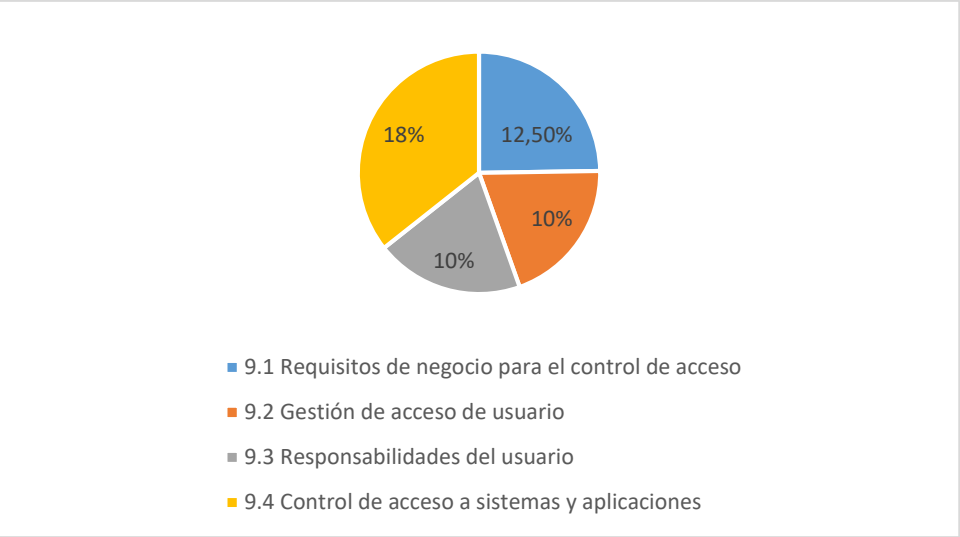
Descripción	Numero de Controles	Ponderación %	Resultado evaluación %
9.1 Requisitos de negocio para el control de acceso	2	25%	12.5%
9.2 Gestión de acceso de usuario	6	35%	10%
9.3 Responsabilidades del usuario	1	10%	0%
9.4 Control de acceso a sistemas y aplicaciones	5	30%	18%
Total	**14**	**100%**	**40.5%**

Nota: tabla que muestra los porcentajes en base a la observación realizada usando ISO27002:2013. Elaboración propia

De los resultados obtenidos podemos representarlos gráficamente como se muestra en la figura 4.

Figura 4

Resultados obtenidos



Nota: Elaboración propia

Una vez obtenidos los datos de la observación realizada en el área de sistematización, es importante conocer la información directa de los responsables del área para lo cual se aplica una entrevista directa a los encargados de funcionamiento e implementación del SIGE, para dicha entrevista se utilizan los controles mencionados por el estándar internacional NIST:800-53.

Es importante mencionar que debido a lo delicado de la información no se pueden mostrar las respuestas a las preguntas planteadas, ya que eso implicaría romper el acuerdo firmado del acta de reserva confidencialidad, se puede observar el formato utilizado en el anexo 1 y los resultados obtenidos se los muestra en la tabla 11 y son los siguientes:

Tabla 11

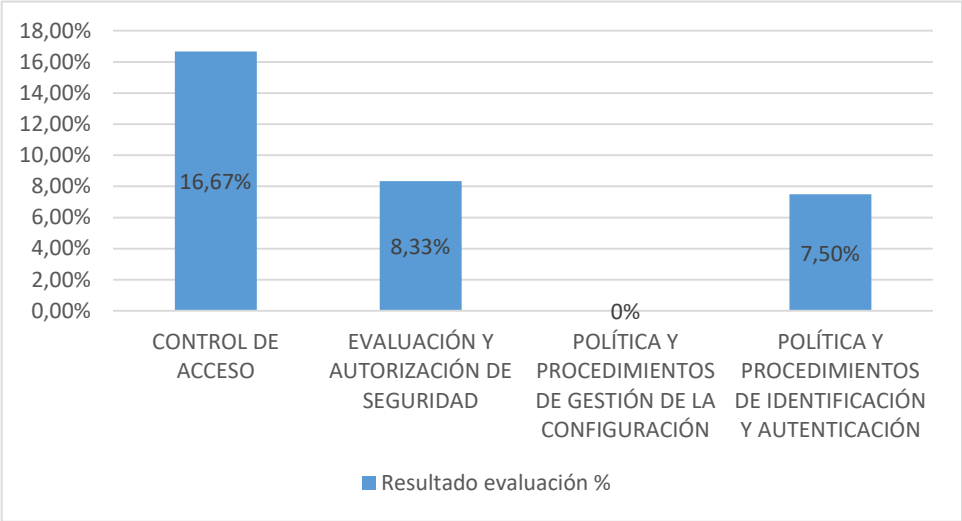
Resultados entrevista

Descripción	Siglas	Nro. Controles	Ponderación %	Resultado evaluación %
CONTROL DE ACCESO	AC	9	30%	16.67%
EVALUACIÓN Y AUTORIZACIÓN DE SEGURIDAD	CA	3	25%	8.33%
POLÍTICA Y PROCEDIMIENTOS DE GESTIÓN DE LA CONFIGURACIÓN	CM	1	15%	0%
POLÍTICA Y PROCEDIMIENTOS DE IDENTIFICACIÓN Y AUTENTICACIÓN	IA	8	30%	7.5%
Total		**21**	**100%**	**32.5%**

Nota: Elaboración propia

Los resultados obtenidos en base a la encuesta realizada se los puede representar gráficamente como se muestra en la figura 5.

Figura 5 *Resultados estadísticos de la entrevista.*



Nota: Elaboración propia

De acuerdo a los datos obtenidos en base a la entrevista y la observación usando los estándares ISO 27002:2013 y NIST:800-53 en el dominio de control de accesos, se puede establecer que los porcentajes arrojados son similares, los dos demuestran que existen controles aplicados, pero no son lo suficientemente fuertes para garantizar la seguridad de la información y se establece que aún deben implementarse otros controles establecidos por las normas para reforzar la seguridad.

Tabla 12

Resultados normas aplicadas

Normas internacionales	**Porcentaje**
ISO27002:2013	40.5%
NIST:800-53	32.5%

Nota: Elaboración propia

Una vez realizados los análisis correspondientes, se puede elaborar un modelo de seguridad informática el mismo que ayudará a aplicar las políticas adecuadas para el manejo correcto de la información y reforzará en gran manera el control de accesos del SIGE.

Propuesta

Los resultados obtenidos pueden considerarse como aceptables ya que los controles utilizados en la actualidad son adecuados, pero aún no son en su totalidad los que garanticen la seguridad de la información, se debe tener un monitoreo constante y aplicar nuevos controles de acuerdo a los estándares establecidos por la ISO 27002:2013 y CSF de NIST. Por lo cual se proponen los siguientes controles:

Prioridades de seguridad (control de accesos)

Control de acceso por usuarios (acceso a la base de datos, servidor, manejo de código fuente)

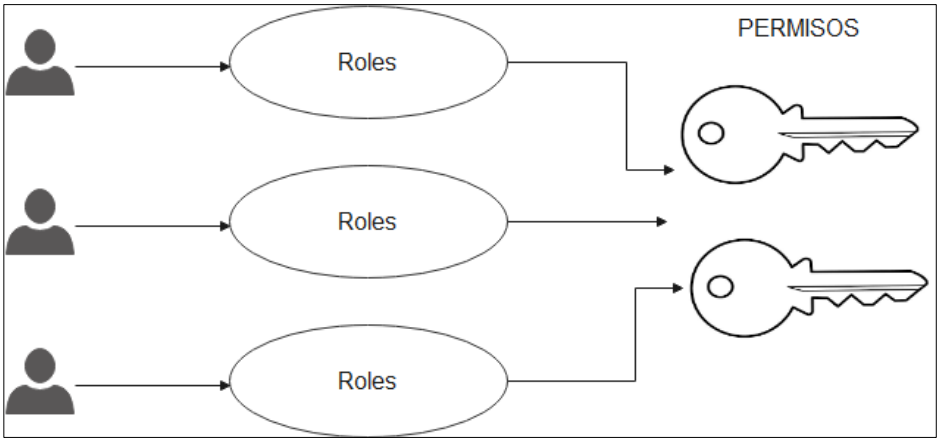
La unidad de sistematización será la que elija cuál de los controles aplicar, los cuales se menciona a continuación:

- **Control de Acceso basado en Roles (RBAC):**

  Se deberá asignar permisos en base a roles en el SIGE para garantizar el acceso solo a partes de la información o accesos al sistema. Cada usuario deberá tener un rol específico para acceso a la información como lo muestra la figura 6.

Figura 6

Control de Acceso basado en Roles



Nota: Elaboración propia

- **Control de Acceso Discrecional (DAC):**

  Para el control de acceso discrecional en el SIGE se deberá aplicar permisos para el acceso a los archivos y directorios, con los permisos correspondientes de lectura y escritura como se muestra en la tabla 13, donde cada usuario tiene establecido un permiso para cada archivo

Tabla 13

Control de Acceso Discrecional

Usuarios	Archivo 1	Archivo 2	Archivo 3
Usuario 1	Lectura	Lectura, escritura	Lectura y ejecución
Usuario 2	Lectura y ejecución	Escritura y ejecución	Sin acceso
Usuario 3	Lectura, escritura y ejecución	Lectura	Lectura

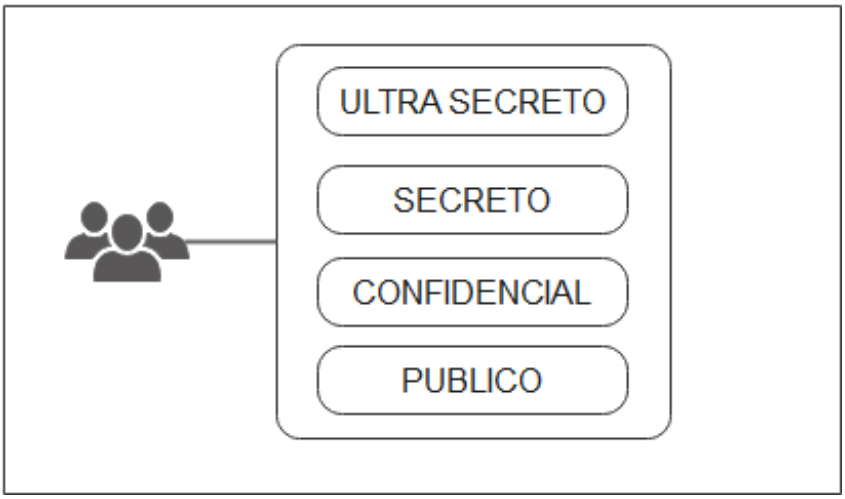
Nota: Elaboración propia

- **Control de Acceso Obligatorio (MAC)**

  El SIGE deberá aplicar controles de acceso en base a etiquetas, las cuales deben verificarse antes de permitir el acceso. La información se clasifica con las etiquetas mostradas en la figura 7 y cada usuario deberá tener un acceso restringido y podrá acceder únicamente a la información proporcionada.

Figura 7

Control de Acceso Obligatorio



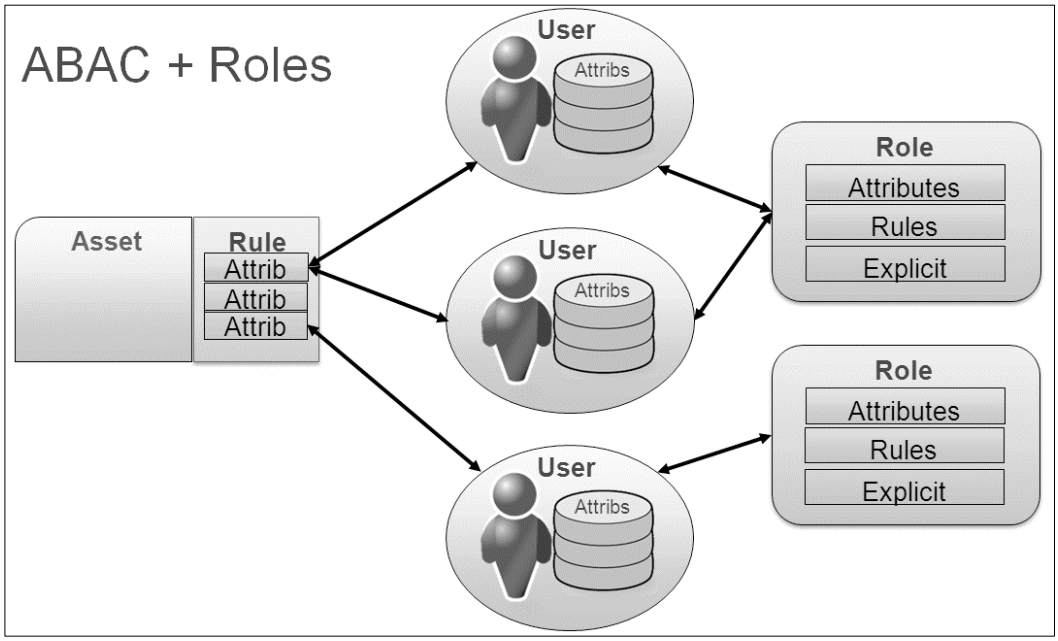
Nota: Elaboración propia

- **Control de Acceso basado en Atributos (ABAC)**

  Se debe aplicar en el SIGE un control de acceso basado en atributos, de manera que el usuario pueda acceder a la información en base a relaciones previamente establecidas ejemplo. Un profesor puede acceder a información de profesor y estudiantes siempre y cuando los roles y los atributos así lo permitan. Gráficamente se lo puede apreciar en la figura 8.

Figura 8

Control de Acceso basado en Atributos



Nota: Tomado de RBAC and ABAC and Roles, Sander(2009)

Auditoría BDD

Se sugiere hacer un análisis de riesgos de la base de datos que maneja el SIGE y en base a estos resultados se establezcan logs de auditoria bajo las siguientes premisas:

- Que usuario accedió a los datos.
- La fecha en que se accedió a los datos.
- Qué tipo de dispositivo utilizó.
- Desde que IP accedió a los datos.
- Qué sentencias se ejecutaron.
- Cómo afectó la ejecución de dichas sentencias a la base de datos.

Restricción Links por rol asociado

El SIGE debe estar en la capacidad de verificar los roles establecidos para determinar si el usuario cuenta con los permisos necesarios para poder ingresar a un formulario específico de la aplicación, de esta manera se garantiza que no pueda acceder a links restringidos para usuarios específicos.

Manejo de Información de alto riesgo

- Identificar las tablas de alto riesgo.

Identificar en el SIGE las tablas de la base de datos que almacenan información confidencial, para la asignación de permisos a los usuarios, con ello se puede controlar el tipo de acceso y permisos de edición de las mismas.

- Creación de tablas temporales.

Para el manejo de información delicada la base de datos del SIGE debe contar con tablas temporales para almacenar la información de manera que permita un análisis previo de la información antes de su paso a producción.

- Módulo de gestión de acceso alto riesgo

Se debe mejorar en el SIGE control de usuarios de manera que se permita obtener información de cada uno de ellos y poder hacer monitoreos de los mismos, este tipo de control debe contar al menos con las siguientes características:

  - Nombre de usuarios
  - Nombre de equipo del cual accede
  - Horarios
  - Permisos (lectura – escritura)
  - Mail de notificación.
  - Roles

Gestión de contraseñas:

Se debe establecer políticas de control en gestión de contraseñas dentro del SIGE bajo las siguientes premisas:

- Establecer cláusulas o normativas para garantizar la privacidad de las contraseñas entregadas a los usuarios.
- Obligación de cambiar la contraseña en el primero ingreso al sistema.
- Cambios de contraseñas periódicas.
- Verificación de contraseñas seguras, evitar el ingreso de contraseñas débiles, similares o ingresadas en fechas anteriores.
- Las contraseñas deben almacenarse en lugares separados a la aplicación

Procedimientos de conexión seguros

Es importante implementar los siguientes controles dentro del SIGE para garantizar el acceso seguro, estos controles se detallan a continuación:

- Establecer controles para inicio de sesión seguros (Doble autenticación). Al momento de iniciar la sesión se deberá enviar un código de confirmación al correo electrónico registrado para validar al acceso.
- Garantizar que los identificadores no se muestren mientras el inicio de sesión no sea realizado con éxito.
- Evitar proporcionar ayudas en el inicio de sesión que puedan dar pistas a usuarios no autorizados.
- Gestión de intentos fallidos con registro de información (fecha, hora, ip).
- El tiempo de sesión debe ser controlado de acuerdo a las necesidades de la institución, los usuarios inactivos deben cerrar su sesión automáticamente.
- Implementación de políticas de acceso en base a horarios, para garantizar el acceso del personal solo en horarios laborales de ser el caso.

Control de acceso al código fuente

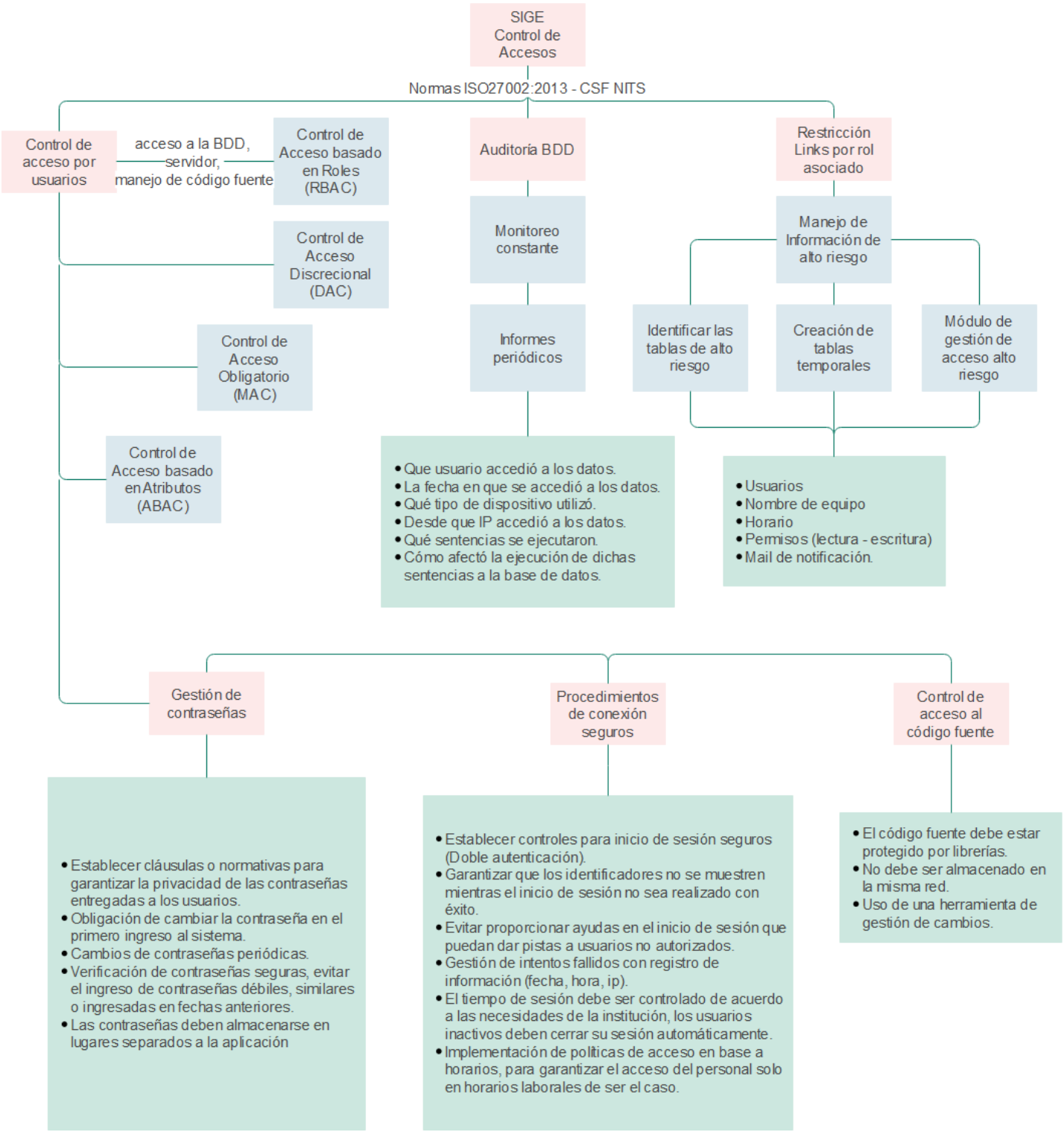
Un aspecto muy importante dentro del área de Sistematización es el manejo del código fuente es cual debe tener los siguientes controles:

- El código fuente debe estar protegido por librerías y el acceso debe ser único para desarrolladores.
- No debe ser almacenado en la misma red.
- Debe hacer uso de una herramienta de gestión de cambios, que maneje el versionamiento con cada cambio realizado y registre en nombre del usuario que lo realizó, de esta manera se llevara un control adecuado del código fuente existente.
- Respaldos periódicos del código fuente.
- Respaldos periódicos de la base de datos.

A continuación, en la figura 9, se resume el modelo propuesto de controles que pueden reforzar el control de accesos del Sistema Integrado de Gestión Estratégica:

Figura 9

Modelo de seguridad control de accesos SIGE



Nota: Elaboración propia

1.4. Matriz de articulación de la propuesta

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

Tabla 14

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
ISO 27002:2013	El estándar internacional ISO 27002:2013 está orientado a la seguridad de la información de cualquier organización, de modo que al sufrir alguna amenaza se minimice al máximo la pérdida o robo de la información.	Uso de metodología de investigación bibliográfica sobre los conceptos básicos de la norma ISO 27002	Fuente bibliográfica	Proporciona los requisitos necesarios para cumplir con los estándares y brindar seguridad en la información	
NIST	El CSF (Cyber Security Framework) de NIST, es un marco para la mejora de la seguridad cibernética, fue desarrollada en los Estados Unidos en el año 2014	Uso de metodología de investigación bibliográfica sobre los conceptos básicos de CSF de NIST	Fuente bibliográfica	Proporciona los requisitos necesarios para cumplir con los estándares y brindar seguridad en la información	

Nota: Elaboración propia

CONCLUSIONES

La ISO27002:2013 es una norma que si bien es cierto hace referencia o propone a ciento catorce controles, la CSF de NIST contiene aspectos que complementan a este estándar como se pudo evidenciar en la revisión de la fundamentación teórica que se realizó.

Una vez que se realizó el mapeo entre la iso27002:2013 y CSF de NIST se identificaron 23 controles que hacen referencia al control de accesos, de los cuales una vez que se validó el Sistema Integrado de Gestión Estratégica cumple con un 40.5% de acuerdo a ISO27002:2013 y un 32.53% para NIST.

Dentro del esquema propuesto y basado en los estándares seleccionados se presenta un conjunto de controles que deben ser aplicados en base a principios básicos y como requisitos mínimos para poder proteger la seguridad de la información.

Dentro del esquema presente se debe considerar la existencia de riesgos no asociados que suelen presentarse como acciones no autorizadas, fallos técnicos, falta de compromiso de los implicados (Usuarios del sistema), afectaciones físicas (infraestructura), falta de control entre otros.

La investigación realizada nos permite demostrar que el Sistema Integrado de Gestión Estratégica cuenta con controles de acceso implementados, pero aún están muy por debajo del nivel que se requiere para un sistema que maneja información importante. Por ello es necesario la implementación de controles adecuados para evitar a futuro algún posible ataque o robo de información.

Es necesario realizar un monitoreo constante de la situación actual del sistema integrado para de esta manera determinar las mejoras que se puedan realizar y lograr con ello una aplicación más fuerte y robusta que brinde seguridad en la información.

Al aplicar las recomendaciones establecidas por los estándares de seguridad ISO 27002:2013 y CSF de NIST se pueden corregir algunos de los problemas que a simple vista son difíciles de detectar y son sumamente importantes dentro de una institución, más aún cuando el manejo de la información es sensible y requiere de ciertos procedimientos para cuidar su integridad, disponibilidad y confidencialidad.

A futuro se podrá evaluar mediante criterio de especialistas el modelo de control de accesos en seguridad informática aplicado ISO 27002 y CSF de NITS, del Sistema Integrado de Gestión Estratégica de la Universidad Israel.

RECOMENDACIONES

Se recomienda realizar un monitoreo constante del control de accesos que se vaya a implementar para evitar los ataques, reforzando constantemente con la investigación de nuevos estándares que se actualizan día tras día.

Se recomienda la implementación de políticas dentro de la institución, las mismas que permitan mejorar las existentes y mantenerse actualizados. Estas políticas deben convertirse en un instrumento de uso constante de manera que su aplicación sea considerada como algo normal dentro de la institución.

Es recomendable continuar con el análisis sobre los riesgos existentes en el control de accesos dentro de la institución para ofrecer una herramienta de calidad. Las revisiones constantes del estado actual servirán de ayuda en la toma de decisiones.

Se recomienda tener un manejo adecuado con las altas y bajas en el sistema, de igual manera con la creación de roles específicos para el acceso a la información. De esta manera se evitará que los usuarios que ya no pertenezcan a la institución todavía tengan acceso a la información y al mismo tiempo evitar que en la base de datos se almacene información que ya no es necesaria.

Se recomienda realizar auditorías constantes con el fin de obtener información actualizada de las posibles instrucciones que se puedan presentar. De esta manera se obtienen datos reales de acceso y permite verificar si se realizó algún ingreso no autorizado con el fin de aplicar las correcciones necesarias para evitar una nueva intrusión.

Es importante continuar con la investigación de normas o estándares que actualmente existen en el mercado de tal manera que permitan fortalecer el Sistema Integrado de Gestión Estratégica.

BIBLIOGRAFÍA

Alejandro Sánchez (2021), Frameworks de ciberseguridad y estándares que debes conocer. https://protegermipc.net/2021/08/19/frameworks-de-ciberseguridad-y-estandares-que-debes-conocer/

Alfredo A. Ortega Sáenz (2021), Protegiendo la Infraestructura Crítica con el NIST Cybersecurity Framework. https://es.linkedin.com/pulse/protegiendo-la-infraestructura-crítica-con-el-nist-ortega-sáenz-1e

Amazon Web Services (2019), Marco de seguridad cibernética NIST (CSF, por sus siglas en inglés). Obtenido de: https://d1.awsstatic.com/whitepapers/es_ES/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Castillo, G. (30 de junio de 2022). Innovación digital 360. Obtenido de Innovación digital 360: https://www.innovaciondigital360.com/big-data/que-son-y-como-funcionan-los-data-center/

Castro, Figueroa, Vera, Álava, Parrales, Murillo, Castillo (2018), INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

CITELIA. (9 de diciembre de 2019). Citelia. Obtenido de Citelio conéctate con nosotros: https://citelia.es/blog/que-es-cloud-computing-y-como-funciona/

Crespo Natalia (2018), La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior. https://repositorio.uta.edu.ec/handle/123456789/27259

Cueva, I. (2015). DISEÑO DE UN PLAN PARA EL TRATAMIENTO DE RIESGOS TECNOLÓGICOS UTILIZANDO LA METODOLOGÍA NIST SP 800–30. DISEÑO DE UN PLAN PARA EL TRATAMIENTO DE RIESGOS TECNOLÓGICOS UTILIZANDO LA METODOLOGÍA NIST SP 800–30. http://repositorio.utmachala.edu.ec/bitstream/48000/5198/1/TTUAIC_2015_ISIST_CD0024.pdf

Equipo editorial. (23 de octubre de 2020). Investigación Bibliográfica: Definición, Tipos, Técnicas. Lifeder. https://www.lifeder.com/37ducación3737ón-bibliografica/.

Erika Reina (2021). Modelo de evaluación del Dominio Control de Acceso de la norma ISO 27002 aplicado al proceso de Gestión de Bases de Datos. https://www.researchgate.net/publication/345792590_Modelo_de_evaluacion_del_Dominio_Control_de_Acceso_de_la_norma_ISO_27002_aplicado_al_proceso_de_Gestion_de_Bases_de_Datos

Fernández Lorena (2022), Control de acceso: qué es y cómo ayuda a proteger nuestros datos. https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

Gallegos Marcos, Galarza Judith, Almuiñas José (2022), Los sistemas de información como sustento a la gestión de la calidad en las Instituciones de Educación Superior. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072022000100137

Guerra Byron (2021), Instituciones educativas en riesgo informático https://www.udla.edu.ec/liderazgo/blog/2021/12/15/instituciones-educativas-en-riesgo-informatico/

HKMEXICO (2022), Principales cambios ISO/IEC 27002:2022 https://www.hkmexico.com/principales-cambios-iso-iec-270022022/

ISO 27001, NORMA ISO 27001. Obtenido de: https://normaiso27001.es

iso27000.es (2013), ISO/IEC 27002:2013. Obtenido de: https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

ISOTools Excellence(2017), *Norma ISO 27002: control de accesos.* https://www.pmg-ssi.com/2017/08/norma-iso-27002-control-de-accesos/

Lourdes Gabriela Álvarez-Lozano,Miguel Santiago Andrade-López(2020), Políticas de Seguridad de la Información bajo la Norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián. https://polodelconocimiento.com/ojs/index.php/es/article/view/2011/html

Molina Oviedo (2020), Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: caso de estudio Universidad Popular del Cesar https://manglar.uninorte.edu.co/handle/10584/10394#page=1

Morales Pablo (2021), Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua – Ecuador. https://www.researchgate.net/publication/352872168_Ciberseguridad_en_plataformas_educativas_institucionales_de_educacion_superior_de_la_provincia_de_Tungurahua_-_Ecuador

NIST (2020), Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Tesis y Másters (2021), ¿Qué es una entrevista? Tipos y clasificación https://tesisymasters.com.ar/que-es-una-entrevista/

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTA

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESPOG | Escuela de Posgrados

Ficha de entrevista para el proyecto de maestría:

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 NITS

La presente ficha de entrevista es para conocer la opinión como experto del área. La información que se alcance será usada exclusivamente para fines académicos y permitirá dar validez al trabajo investigativo.

Nombre del entrevistado:

Área laboral: Años de experiencia:

Preguntas:

¿Cuenta con una política y procedimientos de control de acceso?
¿Existe un proceso para la gestión de cuentas?
¿Cuánta con un control para la aplicación de acceso?
¿Existen roles de Privilegio mínimo?
¿Se controlan los Intentos de inicio de sesión fallidos?
¿Existe una notificación de uso del sistema?
¿Existe una Notificación de inicio de sesión anterior?
¿Cuenta con un Control de sesión concurrente?
¿Se toman decisiones de control de acceso?
¿Se realiza un monitoreo continuo?
¿Existen pruebas de penetración?
¿Existen varias conexiones internas dentro del sistema?
¿Se aplican restricciones de acceso para cambios de contraseña?
¿Existe gestión de identificadores?
¿Existe gestión de autenticadores?

¿Cuenta con identificación y autenticación (usuarios no organizacionales)?
¿Cuenta con identificación y autenticación de servicios?
¿Los procesos de identificación y autenticación son adaptables?
¿Existen procesos de re autenticación?
¿Se realizan pruebas de identidad?
¿Existen roles de liderazgo del Programa de Gestión de Riesgos(altas/bajas)?

Firma:

C.I.

Anexo 2

Entrevista

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESPOG | Escuela de Posgrados

Ficha de entrevista para el proyecto de maestría:

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 NITS

La presente ficha de entrevista es para conocer la opinión como experto del área. La información que se alcance será usada exclusivamente para fines académicos y permitirá dar validez al trabajo investigativo.

Nombre del entrevistado:

Área laboral: Años de experiencia:

Preguntas:

¿Cuenta con una política y procedimientos de control de acceso? ***De acuerdo al SIGE se dispone de una seguridad basado ASP.NET que articula con SQL Server.***
¿Existe un proceso para la gestión de cuentas? ***Se posee un proceso que gestiona las cuentas en base a roles, pero no se dispone un nivel de seguridad alto en dicha gestión.***
¿Cuánta con un control para la aplicación de acceso? ***Existe un formulario de autentificación de usuario, más no una aplicación que maneje y controle el acceso.***
¿Existen roles de Privilegio mínimo? ***Si se dispone de roles y cada uno poseen formularios asignados, mas no privilegios mínimos de seguridad.***
¿Se controlan los Intentos de inicio de sesión fallidos? ***Si se controlan y al tercer intento fallido se bloquea el usuario y adicionalmente le llega un correo electrónico por cada intento fallido.***
¿Existe una notificación de uso del sistema? ***Si, cada vez que se autentifica le llega un correo electrónico con la fecha y hora.***
¿Existe una Notificación de inicio de sesión anterior? ***No se dispone.***
¿Cuenta con un Control de sesión concurrente? ***No se dispone.***
¿Se toman decisiones de control de acceso? ***No se dispone.***
¿Se realiza un monitoreo continuo? ***No se dispone de una política o proceso de monitoreo continuo en el SIGE.***
¿Existen pruebas de penetración? ***No se dispone.***
¿Existen varias conexiones internas dentro del sistema? ***Si por parte de los programadores y QA.***
¿Se aplican restricciones de acceso para cambios de contraseña? ***Existe un formulario para cambio de contraseña, una vez que esté autentificado el usuario en el SIGE.***

¿Existe gestión de identificadores? ***No se dispone.***
¿Existe gestión de autenticadores? ***Se dispone un formulario de autenticación pero no se gestiona.***
¿Cuenta con identificación y autenticación (usuarios no organizacionales)? ***No, solo se crea automáticamente a los usuarios nuevos (estudiantes que van a ingresar a estudiar a la UISRAEL), con el rol de estudiante.***
¿Cuenta con identificación y autenticación de servicios? ***No se dispone.***
¿Los procesos de identificación y autenticación son adaptables? ***No se dispone.***
¿Existen procesos de re autenticación? ***No se dispone.***
¿Se realizan pruebas de identidad? ***El único filtro de identidad se realiza al validar que el número ingresado de la cédula sea válido. Esto en el proceso de inscripción del estudiante (creación de usuario).***
¿Existen roles de liderazgo del Programa de Gestión de Riesgos(altas/bajas)? ***No se dispone.***

Firma:

C.I. 1002807814

Anexo 3

Formato carta reserva confidencialidad

Universidad Israel	UNIDAD DE SISTEMATIZACIÓN	CODIFICACIÓN SI-O-063
	CARTA RESERVA CONFIDENCIALIDAD	FECHA EMISIÓN DOCUMENTO 05-SEP-2022
		NÚMERO REVISIÓN 01

INFORMACION Y MATERIALES CONFIDENCIALES

"La información confidencial" es definida como:

- Información no publica que el editor señala para ser confidencial o
- Aquellas, bajo circunstancias que rodean el acceso, se debe tratar como confidencial, o
- Aquellas que son creadas, producidas y/o escritas por el programador.

La "información confidencial" incluirá sin limitación, todo lo siguiente:

- Datos digitales o impresos, especificaciones, manuales y/o programas similares.
- Del software de los materiales y/o productos y conceptos del código de la programación.
- De software para a venta o la distribución.
- Planes de negocios, planes de comercialización, e información financiera en cualquier formato.
- Nombres de usuarios y/o del software.
- Información de contacto y contraseñas del software.
- Direcciones de páginas web y/o nombre del servidor y contraseñas.
- Nombres de usuarios de la base de datos, contraseñas y/o contenidos.
- Y otra información divulgada oralmente, por e-mail, por escrito o por cualquier otro medio, por el editor al programador.

CLAUSULAS

PRIMERA. Las partes se obligan a no divulgar a terceras partes, la "Información Confidencial", que reciban de la otra, y a darle a dicha información el mismo tratamiento que le darían a la información confidencial de su propiedad.

Para efectos del presente convenio "Información Confidencial" comprende toda la información divulgada por cuales quiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible y que se encuentre claramente marcada como tal al ser entregada a la parte receptora.

SEGUNDA. La parte receptora se obliga a no divulgar la "Información Confidencial" a terceros, sin el previo consentimiento por escrito de la parte divulgante.

TERCERA. La parte receptora se obliga a tomar las precauciones necesarias y apropiadas para mantener como confidencial la "Información Confidencial".

CUARTA. Las partes convienen que en caso que la parte receptora incumpla parcial o totalmente con las obligaciones a su cargo derivadas del presente contrato, la parte receptora será responsable de los daños y perjuicios que dicho incumplimiento llegase a ocasionar a la parte divulgante.

QUINTA. No obstante, lo dispuesto en contrario en este convenio ninguna parte tendrá obligación de mantener como confidencial cualquier información:

1. Que previa a su divulgación fuese conocida por la parte receptora, libre de cualquier obligación de mantenerla confidencial, según se evidencie por documentación en su posesión;
2. Que sea desarrollada o elaborada de manera independiente por o de parte del receptor o legalmente recibida, libre de restricciones, de otra fuente con derecho a divulgarla;
3. Que sea o llegue a ser del dominio público, sin mediar incumplimiento de este convenio por la parte receptora; y
4. Que se reciba de un tercero sin que esa divulgación quebrante o viole una obligación de confidencialidad.

Anexo 3

Tabla de controles NIST SP 800-53

	NIST SP 800-53 CONTROLS	ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AC-1	**Access Control Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	**Account Management**	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	**Access Enforcement**	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	**Information Flow Enforcement**	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	**Separation of Duties**	A.6.1.2
AC-6	**Least Privilege**	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	**Unsuccessful Logon Attempts**	A.9.4.2
AC-8	**System Use Notification**	A.9.4.2
AC-9	**Previous Logon Notification**	A.9.4.2
AC-10	**Concurrent Session Control**	None
AC-11	**Device Lock**	A.11.2.8, A.11.2.9
AC-12	**Session Termination**	None
AC-13	Withdrawn	---
AC-14	**Permitted Actions without Identification or Authentication**	None
AC-15	Withdrawn	---
AC-16	**Security and Privacy Attributes**	None
AC-17	**Remote Access**	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	**Wireless Access**	**A.6.2.1, A.13.1.1, A.13.2.1**
AC-19	**Access Control for Mobile Devices**	A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1
AC-20	**Use of External Systems**	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	**Information Sharing**	None
AC-22	**Publicly Accessible Content**	None
AC-23	**Data Mining Protection**	None
AC-24	**Access Control Decisions**	A.9.4.1*
AC-25	**Reference Monitor**	None
AT-1	**Awareness and Training Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	**Literacy Training and Awareness**	7.3, A.7.2.2, A.12.2.1
AT-3	**Role-Based Training**	A.7.2.2*
AT-4	**Training Records**	None
AT-5	Withdrawn	---
AT-6	**Training Feedback**	None
AU-1	**Audit and Accountability Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	**Event Logging**	None
AU-3	**Content of Audit Records**	A.12.4.1*
AU-4	**Audit Log Storage Capacity**	A.12.1.3
AU-5	**Response to Audit Logging Process Failures**	None
AU-6	**Audit Record Review, Analysis, and Reporting**	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	**Audit Record Reduction and Report Generation**	None
AU-8	**Time Stamps**	A.12.4.4
AU-9	**Protection of Audit Information**	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	**Non-repudiation**	None

AU-11	**Audit Record Retention**	A.12.4.1, A.16.1.7
AU-12	**Audit Record Generation**	A.12.4.1, A.12.4.3
AU-13	**Monitoring for Information Disclosure**	None
AU-14	**Session Audit**	A.12.4.1*
AU-15	Withdrawn	---
AU-16	**Cross-Organizational Audit Logging**	None
CA-1	**Assessment and Authorization Policies and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA-2	**Control Assessments**	A.14.2.8, A.18.2.2, A.18.2.3
CA-3	**Information Exchange**	A.13.1.2, A.13.2.1, A.13.2.2
CA-4	Withdrawn	---
CA-5	**Plan of Action and Milestones**	8.3, 9.2, 10.1*
CA-6	**Authorization**	9.3*
CA-7	**Continuous Monitoring**	9.1, 9.2, A.18.2.2, A.18.2.3*
CA-8	**Penetration Testing**	None
CA-9	**Internal System Connections**	None
CM-1	**Configuration Management Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	**Baseline Configuration**	None
CM-3	**Configuration Change Control**	8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	**Impact Analyses**	A.14.2.3
CM-5	**Access Restrictions for Change**	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	**Configuration Settings**	None
CM-7	**Least Functionality**	A.12.5.1*
CM-8	**System Component Inventory**	A.8.1.1, A.8.1.2
CM-9	**Configuration Management Plan**	A.6.1.1*
CM-10	**Software Usage Restrictions**	A.18.1.2
CM-11	**User-Installed Software**	A.12.5.1, A.12.6.2
CM-12	**Information Location**	None
CM-13	**Data Action Mapping**	None
CM-14	**Signed Components**	None
CP-1	**Contingency Planning Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP-2	**Contingency Plan**	7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1
CP-3	**Contingency Training**	A.7.2.2*
CP-4	**Contingency Plan Testing**	A.17.1.3
CP-5	Withdrawn	---
CP-6	**Alternate Storage Site**	A.11.1.4, A.17.1.2, A.17.2.1
CP-7	**Alternate Processing Site**	A.11.1.4, A.17.1.2, A.17.2.1
CP-8	**Telecommunications Services**	A.11.2.2, A.17.1.2
CP-9	**System Backup**	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	**System Recovery and Reconstitution**	A.17.1.2
CP-11	**Alternate Communications Protocols**	A.17.1.2*
CP-12	**Safe Mode**	None
CP-13	**Alternative Security Mechanisms**	A.17.1.2*
IA-1	**Identification and Authentication Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
IA-2	**Identification and Authentication (Organizational Users)**	A.9.2.1
IA-3	**Device Identification and Authentication**	None
IA-4	**Identifier Management**	A.9.2.1
IA-5	**Authenticator Management**	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
IA-6	**Authentication Feedback**	A.9.4.2

IA-7	**Cryptographic Module Authentication**	A.18.1.5
IA-8	**Identification and Authentication (Non-Organizational Users)**	A.9.2.1
IA-9	**Service Identification and Authentication**	None
IA-10	**Adaptive Identification and Authentication**	None
IA-11	**Re-authentication**	None
IA-12	**Identity Proofing**	None
IR-1	**Incident Response Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR-2	**Incident Response Training**	A.7.2.2*
IR-3	**Incident Response Testing**	None
IR-4	**Incident Handling**	A.16.1.4, A.16.1.5, A.16.1.6
IR-5	**Incident Monitoring**	None
IR-6	**Incident Reporting**	A.6.1.3, A.16.1.2
IR-7	**Incident Response Assistance**	None
IR-8	**Incident Response Plan**	7.5.1, 7.5.2, 7.5.3, A.16.1.1
IR-9	**Information Spillage Response**	None
IR-10	Withdrawn	---
MA-1	**System Maintenance Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA-2	**Controlled Maintenance**	A.11.2.4*, A.11.2.5*
MA-3	**Maintenance Tools**	None
MA-4	**Nonlocal Maintenance**	None
MA-5	**Maintenance Personnel**	None
MA-6	**Timely Maintenance**	A.11.2.4
MA-7	**Field Maintenance**	None
MP-1	**Media Protection Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP-2	**Media Access**	A.8.2.3, A.8.3.1, A.11.2.9
MP-3	**Media Marking**	A.8.2.2
MP-4	**Media Storage**	A.8.2.3, A.8.3.1, A.11.2.9
MP-5	**Media Transport**	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP-6	**Media Sanitization**	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
MP-7	**Media Use**	A.8.2.3, A.8.3.1
MP-8	**Media Downgrading**	None
PE-1	**Physical and Environmental Protection Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE-2	**Physical Access Authorizations**	A.11.1.2*
PE-3	**Physical Access Control**	A.11.1.1, A.11.1.2, A.11.1.3
PE-4	**Access Control for Transmission Medium**	A.11.1.2, A.11.2.3
PE-5	**Access Control for Output Devices**	A.11.1.2, A.11.1.3
PE-6	**Monitoring Physical Access**	None
PE-7	Withdrawn	---
PE-8	**Visitor Access Records**	None
PE-9	**Power Equipment and Cabling**	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE-10	**Emergency Shutoff**	A.11.2.2*
PE-11	**Emergency Power**	A.11.2.2
PE-12	**Emergency Lighting**	A.11.2.2*
PE-13	**Fire Protection**	A.11.1.4, A.11.2.1
PE-14	**Environmental Controls**	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	**Water Damage Protection**	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	**Delivery and Removal**	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	**Alternate Work Site**	A.6.2.2, A.11.2.6, A.13.2.1

PE-18	**Location of System Components**	A.8.2.3, A.11.1.4, A.11.2.1
PE-19	**Information Leakage**	A.11.1.4, A.11.2.1
PE-20	**Asset Monitoring and Tracking**	A.8.2.3*
PE-21	**Electromagnetic Pulse Protection**	None
PE-22	**Component Marking**	A.8.2.2
PE-23	**Facility Location**	A.11.1.4, A.11.2.1
PL-1	**Planning Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	**System Security and Privacy Plans**	7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1
PL-3	Withdrawn	---
PL-4	**Rules of Behavior**	A.7.1.2, A.7.2.1, A.8.1.3
PL-5	Withdrawn	---
PL-6	Withdrawn	---
PL-7	**Concept of Operations**	8.1, A.14.1.1
PL-8	**Security and Privacy Architectures**	A.14.1.1*
PL-9	**Central Management**	None
PL-10	**Baseline Selection**	None
PL-11	**Baseline Tailoring**	None
PM-1	**Information Security Program Plan**	4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	**Information Security Program Leadership Role**	5.1, 5.3, A.6.1.1
PM-3	**Information Security and Privacy Resources**	5.1, 6.2, 7.1
PM-4	**Plan of Action and Milestones Process**	6.1.1, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1
PM-5	**System Inventory**	None
PM-6	**Measures of Performance**	5.3, 6.1.1, 6.2, 9.1,
PM-7	**Enterprise Architecture**	None
PM-8	**Critical Infrastructure Plan**	None
PM-9	**Risk Management Strategy**	4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2
PM-10	**Authorization Process**	9.3, A.6.1.1*
PM-11	**Mission and Business Process Definition**	4.1
PM-12	**Insider Threat Program**	None
PM-13	**Security and Privacy Workforce**	7.2, A.7.2.2*
PM-14	**Testing, Training, and Monitoring**	6.2*
PM-15	**Security and Privacy Groups and Associations**	7.4, A.6.1.4
PM-16	**Threat Awareness Program**	None
PM-17	**Protecting Controlled Unclassified Information on External Systems**	None
PM-18	**Privacy Program Plan**	None
PM-19	**Privacy Program Leadership Role**	None
PM-20	**Dissemination of Privacy Program Information**	None
PM-21	**Accounting of Disclosures**	None
PM-22	**Personally Identifiable Information Quality Management**	None
PM-23	**Data Governance Body**	None
PM-24	**Data Integrity Board**	None
PM-25	**Minimization of Personally Identifiable Information Used in Testing, Training, and Research**	None
PM-26	**Complaint Management**	None
PM-27	**Privacy Reporting**	None
PM-28	**Risk Framing**	4.3, 6.1.2, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3
PM-29	**Risk Management Program Leadership Roles**	5.1, 5.3, 9.2, A.6.1.1
PM-30	**Supply Chain Risk Management Strategy**	4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.2*

PM-31	**Continuous Monitoring Strategy**	4.4, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 9.1, 10.1, 10.2
PM-32	**Purposing**	None
PS-1	**Personnel Security Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	**Position Risk Designation**	None
PS-3	**Personnel Screening**	A.7.1.1
PS-4	**Personnel Termination**	A.7.3.1, A.8.1.4
PS-5	**Personnel Transfer**	A.7.3.1, A.8.1.4
PS-6	**Access Agreements**	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	**External Personnel Security**	A.6.1.1, A.7.2.1*
PS-8	**Personnel Sanctions**	7.3, A.7.2.3
PS-9	**Position Descriptions**	A.6.1.1
PT-1	**Personally Identifiable Information Processing and Transparency Policy and Procedures**	None
PT-2	**Authority to Process Personally Identifiable Information**	None
PT-3	**Personally Identifiable Information Processing Purposes**	None
PT-4	**Consent**	None
PT-5	**Privacy Notice**	None
PT-6	**System of Records Notice**	None
PT-7	**Specific Categories of Personally Identifiable Information**	None
PT-8	**Computer Matching Requirements**	None
RA-1	**Risk Assessment Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA-2	**Security Categorization**	A.8.2.1
RA-3	**Risk Assessment**	6.1.2, 8.2, A.12.6.1*
RA-4	Withdrawn	---
RA-5	**Vulnerability Monitoring and Scanning**	A.12.6.1*
RA-6	**Technical Surveillance Countermeasures Survey**	None
RA-7	**Risk Response**	6.1.3, 8.3, 10.1
RA-8	**Privacy Impact Assessments**	None
RA-9	**Criticality Analysis**	A.15.2.2*
RA-10	**Threat Hunting**	None
SA-1	**System and Services Acquisition Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	**Allocation of Resources**	None
SA-3	**System Development Life Cycle**	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	**Acquisition Process**	8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	**System Documentation**	7.5.1, 7.5.2, 7.5.3, A.12.1.1*
SA-6	Withdrawn	---
SA-7	Withdrawn	---
SA-8	**Security Engineering Principles**	A.14.2.5
SA-9	**External System Services**	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	**Developer Configuration Management**	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	**Developer Testing and Evaluation**	A.14.2.7, A.14.2.8
SA-12	Withdrawn	---
SA-13	Withdrawn	---
SA-14	Withdrawn	---
SA-15	**Development Process, Standards, and Tools**	A.6.1.5, A.14.2.1
SA-16	**Developer-Provided Training**	None

SA-17	**Developer Security and Privacy Architecture and Design**	A.14.2.1, A.14.2.5
SA-18	Withdrawn	---
SA-19	Withdrawn	---
SA-20	**Customized Development of Critical Components**	None
SA-21	**Developer Screening**	A.7.1.1
SA-22	**Unsupported System Components**	None
SA-23	**Specialization**	None
SC-1	**System and Communications Protection Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SC-2	**Separation of System and User Functionality**	None
SC-3	**Security Function Isolation**	None
SC-4	**Information In Shared System Resources**	None
SC-5	**Denial-of Service-Protection**	None
SC-6	**Resource Availability**	None
SC-7	**Boundary Protection**	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
SC-8	**Transmission Confidentiality and Integrity**	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
SC-9	Withdrawn	---
SC-10	**Network Disconnect**	A.13.1.1
SC-11	**Trusted Path**	None
SC-12	**Cryptographic Key Establishment and Management**	A.10.1.2
SC-13	**Cryptographic Protection**	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
SC-14	Withdrawn	---
SC-15	**Collaborative Computing Devices and Applications**	A.13.2.1*
SC-16	**Transmission of Security and Privacy Attributes**	None
SC-17	**Public Key Infrastructure Certificates**	A.10.1.2
SC-18	**Mobile Code**	None
SC-19	Withdrawn	None
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**	None
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**	None
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	None
SC-23	**Session Authenticity**	None
SC-24	**Fail in Known State**	None
SC-25	**Thin Nodes**	None
SC-26	**Decoys**	None
SC-27	**Platform-Independent Applications**	None
SC-28	**Protection of Information at Rest**	A.8.2.3*
SC-29	**Heterogeneity**	None
SC-30	**Concealment and Misdirection**	None
SC-31	**Covert Channel Analysis**	None
SC-32	**System Partitioning**	None
SC-33	Withdrawn	---
SC-34	**Non-Modifiable Executable Programs**	None
SC-35	**External Malicious Code Identification**	None
SC-36	**Distributed Processing and Storage**	None
SC-37	**Out-of-Band Channels**	None
SC-38	**Operations Security**	A.12.x
SC-39	**Process Isolation**	None

SC-40	**Wireless Link Protection**	None
SC-41	**Port and I/O Device Access**	None
SC-42	**Sensor Capability and Data**	A.11.1.5*
SC-43	**Usage Restrictions**	None
SC-44	**Detonation Chambers**	None
SC-45	**System Time Synchronization**	None
SC-46	**Cross Domain Policy Enforcement**	None
SC-47	**Alternate Communications Paths**	None
SC-48	**Sensor Relocation**	None
SC-49	**Hardware-Enforced Separation and Policy Enforcement**	None
SC-50	**Software-Enforced Separation and Policy Enforcement**	None
SC-51	**Hardware-Based Protection**	None
SI-1	**System and Information Integrity Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SI-2	**Flaw Remediation**	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SI-3	**Malicious Code Protection**	A.12.2.1
SI-4	**System Monitoring**	None
SI-5	**Security Alerts, Advisories, and Directives**	A.6.1.4*
SI-6	**Security and Privacy Function Verification**	None
SI-7	**Software, Firmware, and Information Integrity**	None
SI-8	**Spam Protection**	None
SI-9	Withdrawn	---
SI-10	**Information Input Validation**	None
SI-11	**Error Handling**	None
SI-12	**Information Management and Retention**	None
SI-13	**Predictable Failure Prevention**	None
SI-14	**Non-Persistence**	None
SI-15	**Information Output Filtering**	None
SI-16	**Memory Protection**	None
SI-17	**Fail-Safe Procedures**	None
SI-18	**Personally Identifiable Information Quality Operations**	None
SI-19	**De-identification**	None
SI-20	**Tainting**	None
SI-21	**Information Refresh**	None
SI-22	**Information Diversity**	None
SI-23	**Information Fragmentation**	None
SR-1	**Supply Chain Risk Management Policy and Procedures**	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.15.1.1, A.18.1.1, A.18.2.2
SR-2	**Supply Chain Risk Management Plan**	A.14.2.7*
SR-3	**Supply Chain Controls and Processes**	A.15.1.2, A.15.1.3*
SR-4	**Provenance**	A.14.2.7*
SR-5	**Acquisition Strategies, Tools, and Methods**	A.15.1.3
SR-6	**Supplier Assessments and Reviews**	A.15.2.1
SR-7	**Supply Chain Operations Security**	A.15.2.2*
SR-8	**Notification Agreements**	None
SR-9	**Tamper Resistance and Detection**	None
SR-10	**Inspection of Systems or Components**	None
SR-11	**Component Authenticity**	None
SR-12	**Component Disposal**	None

Nota: asignación de controles NIST 800-53 vs ISO27001, tomado de csrc.nist.gov (2020)