UNIVERSIDAD DON BOSCO

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Diseño de un Sistema de Gestión de Seguridad de la Información para la Cooperativa Financiera SIHUACOOP DE R.L.

PRESENTADO POR

Kevin Omar Álvarez Hernández

Jaime Alfredo Avilés Fermán

Rodrigo Antonio Ayala Meléndez

ASESOR

Mg. Leonardo Castillo

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Agosto 2023

RESUMEN

Las empresas siempre buscan resguardar sus activos, así como la información sin importar si esta se encuentra en medios físicos o digitales. Dado el auge actual de cuarta revolución industrial que ha impulsado el crecimiento tecnológico para ofrecer canales más convenientes para los usuarios a través de Internet; el problema es que estas nuevas vías propician nuevas amenazas y vulnerabilidades para la preciada información de las organizaciones.

La información financiera y personal de los clientes, así como los activos de organización, son valiosos y deben ser protegidos contra estas nuevas posibles amenazas, como ciberataques, fraudes o robos. La implementación de la norma ISO 27001 es una forma efectiva de proteger la información y los activos, y garantizar que se cumplan requisitos legales y regulatorios en materia de protección de datos.

La norma ISO 27001 es un estándar internacional para la gestión de la seguridad de la información que ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de sus datos. Implementar esta norma ayudaría a identificar riesgos y amenazas que las organizaciones enfrentan y a implementar medidas para reducir estos riesgos.

El presente trabajo se basa en diseñar un Sistema de Gestión de Seguridad de la Información (SGSI), para la Cooperativa de Ahorro y Crédito SIHUACOOP DE R.L., utilizando como base la norma internacional ISO 27001:2022. Tomando en cuenta esta norma internacional ampliamente reconocida, asimismo la situación actual y la problemática en la cooperativa financiera, se pretende determinar e identificar la forma efectiva de gestionar los riesgos que existan en los diferentes procesos de la institución, de tal forma que permita adecuar las necesidades y requerimientos a estándares internacionales y leyes nacionales que permitan garantizar la confidencialidad, integridad y disponibilidad de la información.

Con el diseño del Sistema de Gestión de Seguridad de la Información, se pretende lograr que la institución se alinee con los objetivos estratégicos de la cooperativa con los objetivos de controles de la norma internacional para la gestión de los riesgos y vulnerabilidades, identificando sus riesgos a través de controles en los activos y procesos de la cooperativa.

Índice

Índice de Figuras

Índice de Tablas

Introducción

La evolución constante y acelerada de la tecnología trae consigo muchos retos atribuibles a la seguridad y protección de datos ya que esto acarrea riesgos y vulnerabilidades las cuales debemos de conocer, controlar, mitigar, aceptar o transferir. En tiempo de pandemia se expusieron más los datos debido a la colaboración remota de los trabajadores y con esto la manera de proteger los datos. Esto cambio positivamente el interés que debemos de darle a la seguridad de los sistemas de información y activos digitales de las organizaciones. Es por lo anterior que se vuelve fundamental y de rigor contar con un sistema de gestión de seguridad de la información (SGSI) que permita salvaguardar los recursos informáticos, ayudando a cumplir los objetivos corporativos. La gestión para la seguridad debe ser conocida por toda la organización y así garantizar que los riesgos sean identificados, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La cooperativa financiera SIHUACOOP DE R.L. manifiesta la importancia de la información y la considera que es uno de los activos más valiosos que poseen por lo cual comprende que es necesario que la cooperativa tenga una adecuada gestión de sus activos y recursos de información con el fin de asegurar el debido tratamiento de la información. En este sentido el proyecto comprende el evaluar el nivel de madurez que la cooperativa tiene en materia de gestión y seguridad de la información que nos permitirá identificar las vulnerabilidades, amenazas y riesgos a los que se encuentran expuestos y a la vez nos servirá como parámetro para diseñar un Sistema de Gestión de Seguridad de la Información.

Capítulo I: Generalidades del proyecto

Antecedentes

Cooperativismo Internacional

El cooperativismo es un modelo económico y social basado en la cooperación y el trabajo en equipo entre personas que tienen intereses y necesidades comunes. El concepto de cooperativa se remonta a la década de 1840, pero los antecedentes históricos del cooperativismo se pueden encontrar en muchas sociedades y culturas antiguas.

En la Edad Media, las guildas y cofradías de artesanos se formaron para proteger los derechos e intereses económicos de sus miembros, y se caracterizaron por su espíritu de cooperación y ayuda mutua. En la época colonial, las organizaciones gremiales y mutualistas de los trabajadores de Europa y América Latina también promovieron la cooperación y la solidaridad entre sus miembros.

El primer registro histórico conocido de una cooperativa moderna fue la sociedad de tejedores de Rochdale, fundada en 1844 en Inglaterra. Los miembros de la sociedad se unieron para comprar materias primas juntos y vender sus productos terminados a precios justos, lo que les permitió obtener mayores beneficios y mejorar su calidad de vida.

El movimiento cooperativo se expandió rápidamente a través de Europa y América del Norte durante el siglo XIX, y se convirtió en una alternativa popular al capitalismo industrial. Las cooperativas se formaron en muchos sectores de la economía, como la agricultura, la industria, el comercio y los servicios, y se basaron en los principios de democracia, igualdad y solidaridad entre los miembros.

En la actualidad, el cooperativismo se ha convertido en una fuerza importante en todo el mundo, con millones de cooperativas y miles de millones de miembros. Las cooperativas se han demostrado como una herramienta efectiva para promover el desarrollo económico y social, mejorar la calidad de vida de las personas y fomentar la participación ciudadana y la democracia económica.

Cooperativismo Nacional

En El Salvador, el cooperativismo comenzó a principios del siglo XX, pero tuvo un desarrollo significativo a partir de la década de 1960. Durante esta época, la economía salvadoreña estaba dominada por grandes empresas y terratenientes, y la mayoría de la población rural y urbana se encontraba en una situación de pobreza y exclusión social.

En este contexto, varias organizaciones comenzaron a promover el cooperativismo como una alternativa económica y social para los trabajadores y los pequeños productores. Una de las primeras cooperativas en El Salvador fue la Cooperativa de Ahorro y Crédito de Santa Ana, fundada en 1947. Sin embargo, fue en la década de 1960 cuando se formaron las primeras cooperativas agrícolas y de consumo, impulsadas por organizaciones sindicales y populares.

En 1969 se fundó la Federación de Cooperativas Agrícolas de El Salvador (FEDECACES), que se convirtió en una fuerza importante en el desarrollo del cooperativismo en el país. FEDECACES se enfocó en el desarrollo agrícola y la comercialización de productos de sus cooperativas miembros, así como en la educación y capacitación de los trabajadores y los pequeños productores.

En la década de 1980, durante la guerra civil en El Salvador, el movimiento cooperativo enfrentó grandes desafíos debido a la represión política y la violencia en el país. Muchas cooperativas fueron cerradas o destruidas, y sus miembros fueron perseguidos o desplazados.

Sin embargo, después del conflicto armado, el cooperativismo resurgió con fuerza en El Salvador. En 1993 se creó la Ley de Cooperativas, que reconoció oficialmente el papel de las cooperativas en la economía del país y estableció un marco legal para su funcionamiento.

En la actualidad, el cooperativismo sigue siendo una alternativa importante para los trabajadores, los pequeños productores y los consumidores en El Salvador. Existen cooperativas en diferentes sectores de la economía, como la agricultura, el comercio, los servicios y las finanzas, y se han convertido en un actor clave en la promoción del desarrollo sostenible y la inclusión social en el país.

Situación actual de la Cooperativa

El análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es una herramienta ampliamente utilizada para evaluar la posición estratégica que una organización posee. A través de este análisis, se busca comprender tanto los factores internos como externos que pueden influir en el desempeño de la organización.

El objetivo de este análisis FODA es identificar los factores clave que influyen en el rendimiento y la posición competitiva de la entidad financiera en relación con Tecnología de Información. Esto permitirá a la entidad tomar decisiones informadas y desarrollar estrategias efectivas para alcanzar sus objetivos.

Es importante destacar que el análisis FODA no proporciona soluciones directas, pero sí brinda una base sólida para la toma de decisiones estratégicas. En este caso, nos ayudara a tener una idea de la situación actual, este análisis FODA fue desarrollado en comunicación con el área de Tecnología de SIHUACOOP DE R.L.

Tabla 1. Análisis FODA de SIHUACOOP DE R.L.

Fortalezas	Oportunidades
• Aplicaciones orientadas a entorno web, facilitado el acceso a estos servicios. • Desarrollo Interno, cambios pueden realizarse en un tiempo prudencial y no se está limitado por un proveedor. • Copias de seguridad en la nube. • Uso de Firewall en todas las agencias y central. Además del uso de Firewall para Aplicaciones Web (WAF, por sus siglas en Ingles) • Conectividad a través de VPN entre agencias y central. • Disponibilidad de servicios de TI: Virtualización de servidores, Telefonía IP y Servidor de correo.	• Creación de nuevos canales digitales para optimizar atención al cliente y servicios ofrecidos. • Alianzas estratégicas con otros negocios, como FEDECACES. • Nuevas agencias, posibilidad de expandir • Mejora de aplicación móvil y servicios en línea ofrecidos.
Debilidades	**Amenazas**
• Estructura de TI plana, falta de Gobierno de TI. • Presupuesto limitado para proyectos de TI • Falta de respaldo de electricidad en agencias. • Base de datos no normalizada. • Carencia en adopción de normas. • Poco personal para el numero de responsabilidades actuales de TI.	• Obsolescencia en servicios de TI. • Gestión de Seguridad deficiente. • Crecimiento cibercrimen a nivel nacional (Phishing[1], Virus, Hackers[2])

[1] Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjeta de crédito.
[2] Personas con habilidades en manejo de computadoras que buscan comprometer dispositivos digitales.

Seguridad de la información

La seguridad de la información ha sido una preocupación desde hace mucho tiempo. En los primeros días de la comunicación electrónica, la seguridad se centraba principalmente en proteger los sistemas y redes de los ataques externos. Con el aumento de la cantidad de información personal y empresarial almacenada y compartida digitalmente, la seguridad de la información se ha convertido en una prioridad crítica en la era digital.

Los antecedentes de la seguridad de la información se remontan a la época de la criptografía, la técnica de codificación de mensajes para mantenerlos seguros de los que no debían verlos. Los primeros sistemas de cifrado se remontan a la Antigua Grecia, donde el escítala se utilizó para proteger las comunicaciones militares. A lo largo de la historia, la criptografía ha evolucionado y se ha utilizado en varios conflictos militares y guerras, incluidas las dos guerras mundiales.

A mediados del siglo XX, con el aumento de las computadoras y las redes, la seguridad de la información se centró en la protección de los sistemas informáticos y las comunicaciones de red. En la década de 1970, se desarrollaron las primeras técnicas de encriptación de datos, como DES (Data Encryption Standard) y RSA (Rivest, Shamir y Adleman), lo que permitió proteger la información transmitida a través de redes digitales.

Con el aumento de la dependencia de las tecnologías de la información y la comunicación en la sociedad actual, la seguridad de la información ha evolucionado para incluir la protección de datos personales y empresariales, la prevención de la piratería informática y el cibercrimen, y la garantía de la privacidad en línea.

Garantizar la protección de la información, uno de los activos más valiosos hoy en día, requiere una estructura organizativa interna sólida en las instituciones, ya que es necesario evaluar diariamente su importancia. En el pasado, las organizaciones guardaban todos los datos en formato físico, lo que presentaba riesgos de pérdida debido a desastres naturales, incendios y robos. Con la llegada de las computadoras y las redes, se aceleró el procesamiento y la digitalización de los datos, lo que permitió un almacenamiento más eficiente y una divulgación más fácil. A partir de los años 80, se volvió más importante proteger los activos que procesan información importante, ya que surgieron nuevas amenazas en la década de los 90.

Para garantizar la protección de la información, es necesario considerar diversos aspectos técnicos, legales, ambientales y físicos. Esto incluye temas como hardware, software, códigos, lenguaje de datos y seguridad física y ambiental. Este campo ofrece una amplia variedad de especializaciones, como la auditoría de sistemas de información y los sistemas de gestión de seguridad.

A lo largo de la historia, la información ha sido importante para los seres humanos. En el pasado, la información valiosa se guardaba en objetos sofisticados y se almacenaba en lugares de difícil acceso. Solo las personas autorizadas podían acceder a ella. Con el tiempo, surgieron nuevas técnicas de procesamiento y almacenamiento, así como redes de comunicación, que ofrecen nuevas opciones para proteger este activo valioso.

Tabla 2. Primeros virus informáticos conocidos antes del 2000.

Virus	Año de aparición	Descripción
Brain	1986	Fue el primer virus de MS-DOS que se propagó por todo el mundo. Su efecto fue principalmente para reducir el rendimiento del sistema infectado y ocultar directorios.
Jerusalem	1987	También conocido como "viernes 13", este virus se propagó rápidamente en Israel, pero también se extendió a otros países. Una vez que se activaba, el virus eliminaba cualquier programa que el usuario intentara ejecutar el viernes 13, lo que hacía que la computadora dejara de funcionar.
Cascade	1987	Este virus fue uno de los primeros virus en infectar sistemas DOS y era conocido por su complejidad en el código. Una vez que el virus se activaba, se movía a través de los archivos del sistema y se copiaba a sí mismo en el directorio raíz.
Stoned	1987	El virus Stoned infectó el sector de arranque de los discos duros de las computadoras y se activaba cada vez que se iniciaba la computadora. Una vez activado, el virus mostraba un mensaje que decía "Tu computadora está ahora apedreada".
Michelangelo	1991	Este virus se activaba el 6 de marzo, que era el cumpleaños del famoso artista renacentista Michelangelo. El virus se ocultaba en el disco duro de la

		computadora y luego se activaba el 6 de marzo, donde borraba todo el contenido del disco duro.
Melissa	1999	Fue uno de los primeros virus de correo electrónico. El virus se propagaba por correo electrónico y, una vez activado, enviaba una copia de sí mismo a las primeras 50 direcciones de correo electrónico encontradas en la libreta de direcciones de la víctima.
CIH (Chernobyl)	1998	Nombrado en honor a la explosión nuclear de Chernobyl en 1986, este virus se activaba el 26 de abril, aniversario de la tragedia. El virus destruía datos en el disco duro y corrompía la memoria de la computadora.
Bubbleboy	1999	Otro virus de correo electrónico, el virus Bubbleboy se propagaba a través del correo electrónico sin la necesidad de que el usuario abriera un archivo adjunto. Una vez activado, el virus permitía a un atacante tomar el control de la computadora de la víctima.
ExploreZip	1999	Este virus se propagaba a través de archivos ZIP infectados que se enviaban por correo electrónico. Una vez que se activaba, el virus eliminaba archivos importantes del sistema y se copiaba a sí mismo en todos los archivos ZIP que se encontraban en la computadora.
LoveLetter (ILOVEYOU)	2000	Uno de los virus más destructivos de la historia, se propagaba por correo electrónico y borraba archivos en el sistema.

En la actualidad, la seguridad de la información es una disciplina interdisciplinaria que se centra en proteger la información y los sistemas informáticos contra los ataques cibernéticos, el malware[3], el robo de identidad y otros riesgos en línea.

[3] Malware o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

Historia de la ISO

Las Normas ISO (International Organization for Standardization) son un conjunto de estándares internacionales que establecen los requisitos y las mejores prácticas en una amplia variedad de áreas, desde la calidad y la seguridad hasta el medio ambiente y la gestión de la información. El objetivo principal de estas normas es proporcionar un marco de referencia para la mejora continua de los procesos y prácticas empresariales.

Los antecedentes de las normas ISO se remontan a 1946, cuando se fundó la Organización Internacional de Normalización en Ginebra, Suiza. La organización se creó con el objetivo de desarrollar estándares internacionales para la industria y el comercio con el fin de facilitar el comercio y mejorar la calidad de los productos y servicios.

En 1987, la ISO publicó la norma ISO 9001, que establece los requisitos para un sistema de gestión de la calidad (SGC). Desde entonces, se han desarrollado y publicado varias otras normas ISO relacionadas con la calidad, incluidas la ISO 14001 para gestión ambiental, la ISO 45001 para salud y seguridad ocupacional, y la ISO 27001 para seguridad de la información.

Las normas ISO han evolucionado para convertirse en un conjunto de estándares reconocidos a nivel mundial, y su adopción puede mejorar la calidad de los productos y servicios, aumentar la eficiencia y la productividad, y mejorar la gestión de riesgos y la toma de decisiones empresariales.

La importación de las normas ISO a nivel internacional se ha convertido en una práctica común en el mundo empresarial. La adopción de estas normas puede ayudar a las empresas a mejorar la calidad de sus productos y servicios, aumentar la eficiencia y la productividad, y mejorar la gestión de riesgos y la toma de decisiones empresariales.

La certificación de una empresa en una norma ISO específica significa que ha implementado y cumple con los requisitos establecidos por esa norma, lo que puede mejorar la confianza del cliente y la credibilidad de la empresa. Además, la certificación puede abrir nuevas oportunidades de negocio, ya que muchas organizaciones buscan trabajar con empresas que están certificadas en ciertas normas ISO.

Sin embargo, la certificación en una norma ISO no es un proceso fácil ni rápido. Requiere una planificación cuidadosa, una implementación rigurosa y una auditoría externa para verificar el cumplimiento de los requisitos de la norma. Además, el costo

de obtener la certificación puede ser significativo, especialmente para empresas más pequeñas.

A pesar de estos desafíos, la adopción de normas ISO y la certificación pueden ser una inversión valiosa para cualquier empresa que busque mejorar sus prácticas y procesos empresariales.

ISO27001

La norma ISO 27001 es una norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), se originó a partir de la norma BS 7799 / ISO 17799, reconocida internacionalmente en el dominio y muy utilizada para la redacción de las políticas de seguridad.

La norma BS 7799 / ISO 17799 fue publicada en dos partes:

ISO / CEI 17799 Parte 1

Código de buenas prácticas relativas a la gestión de la seguridad de la información. Es una guía que contiene consejos y recomendaciones que permite asegurar la seguridad de la información de la empresa dentro de los diez dominios de aplicación.

BS 7799 fue un estándar publicado originalmente por BSI Group en 1995. Fue escrito por el Departamento de Comercio e Industria del Gobierno del Reino Unido y constaba de varias partes.

BS 7799 Parte 2

Las especificaciones relativas a la gestión de la seguridad de la información proponen recomendaciones con el fin de establecer un marco eficaz de gestión de la seguridad de la información. En el momento de una auditoría, es el documento que sirve de guía de evaluación para la certificación.

BS 7799-2 publicada por el “British Standards Institution (BSI)” por primera vez en 1998 donde estableció los de requisitos para certificar un SGSI. En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas propuestas por Organización Internacional de Normalización (ISO) y se publicó por primera vez en el año 2005. Desde entonces, se ha convertido en una norma ampliamente utilizada por las organizaciones de todo el mundo para mejorar la seguridad de la información y protegerla de amenazas internas y externas.

La norma ISO 27001 se basa en el ciclo de mejora continua PDCA (Planificar, Hacer, Verificar, Actuar) y proporciona un enfoque sistemático y estructurado para la gestión de la seguridad de la información. La norma establece requisitos para la gestión de riesgos de seguridad de la información, la selección y aplicación de controles de seguridad, la gestión de incidentes de seguridad y la mejora continua del SGSI.

- **Plan** *(planificar)*: es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **Do** *(hacer)*: es una fase que envuelve la implantación y operación de los controles.
- **Check** *(controlar)*: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act** *(actuar)*: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Ilustración 1. Ciclo de vida ISO 27001.

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

La norma ISO 27001 se aplica a cualquier tipo de organización, independientemente de su tamaño o sector de actividad, y se puede adaptar a las necesidades específicas de cada organización. La implementación de la norma ISO 27001 puede proporcionar varios beneficios a las organizaciones, como una mayor confianza de los clientes y las partes interesadas, una mejor gestión de los riesgos de seguridad de la información,

una mayor eficiencia en los procesos empresariales y la reducción de costos asociados a incidentes de seguridad. Además, la implementación de la norma ISO 27001 puede ayudar a las organizaciones a cumplir con las regulaciones y requisitos legales relacionados con la seguridad de la información.

Sin embargo, la implementación de la norma ISO 27001 no es una tarea fácil. Requiere un compromiso de la dirección de la organización, una planificación cuidadosa, una implementación rigurosa y una auditoría externa para verificar el cumplimiento de los requisitos de la norma.

Norma ISO 27001 en El Salvador

La OSN (Organismo Salvadoreño de Normalización) es un organismo público no estatal encargado de promover y coordinar la normalización en El Salvador. Fue creado en 2001 mediante el Decreto Legislativo N° 876 con el fin de mejorar la competitividad del país a través del fomento de la calidad, la seguridad y la protección del medio ambiente.

La OSN es miembro activo de la ISO (Organización Internacional de Normalización) y como tal, está comprometido con la promoción de la adopción de normas ISO en el país. Para ello, la OSN se encarga de difundir y promover la importancia de las normas ISO en distintos sectores y empresas del país, así como de brindar capacitaciones y asesorías para la implementación de sistemas de gestión basados en normas ISO.

En relación específica a la norma ISO 27001, la OSN ha impulsado su adopción en El Salvador a través de la creación de comités técnicos especializados en seguridad de la información, conformados por expertos en el tema de diferentes instituciones públicas y privadas del país. Además, la OSN ha promovido la capacitación y asesoría en la implementación de sistemas de gestión de seguridad de la información basados en la norma ISO 27001 en diferentes empresas del país.

Además de la OSN, otras entidades en El Salvador también han promovido la adopción de la norma ISO 27001. Por ejemplo, el Ministerio de Seguridad Pública y Justicia, a través de la Dirección de Información y Tecnología, ha fomentado la implementación de sistemas de seguridad de la información en las instituciones del sector público.

En el ámbito empresarial, diversas organizaciones han implementado la norma ISO 27001 como parte de su estrategia de gestión de riesgos y seguridad de la información. Algunas empresas en El Salvador que han obtenido la certificación ISO 27001 son: Banco Agrícola, Tropigas, Grupo Q, Crediservicios, entre otras.

Formulación del problema

Descripción del problema

La cooperativa SIHUACOOP DE R.L. se enfrenta a diversos desafíos en cuanto a la seguridad de la información, incluyendo la protección de datos de sus clientes y la gestión de la información interna. Actualmente, carece de un enfoque estructurado y sistemático para abordar estos desafíos, lo que puede resultar en vulnerabilidades y riesgos de seguridad que podrían afectar su reputación y operaciones.

La implementación de un SGSI en SIHUACOOP DE R.L. permitirá establecer una metodología sólida y ordenada para abordar los riesgos de seguridad de la información, adaptándose de forma efectiva a los cambios en el entorno, los riesgos y las tecnologías emergentes. Con la adopción de esta norma internacional, la cooperativa fortalecerá su capacidad para proteger la información sensible, tanto de sus clientes como de su propia operación, generando confianza y brindando un servicio seguro y confiable.

Además, la implementación de la ISO 27001 contribuirá a mejorar la eficiencia operativa de SIHUACOOP DE R.L., al establecer controles y procedimientos adecuados para prevenir y mitigar incidentes de seguridad de la información, así como para responder de manera efectiva en caso de que ocurran. Esto se traducirá en una mayor resiliencia de la cooperativa frente a posibles amenazas y un cumplimiento normativo más riguroso.

Planteamiento de problema

En la actualidad, las cooperativas en todo el mundo han surgido gracias a tecnologías nuevas que han permitido dar un giro en la forma como se hacen los negocios, de igual manera han incrementado los riesgos para ellas, de igual manera se exponen a nuevas amenazas. ¿De qué manera un enfoque basado en procesos permite diseñar el SGSI (Sistema de Gestión de Seguridad de la Información) para garantizar la confidencialidad, integridad y disponibilidad de la información en la Cooperativa SIHUACOOP DE R.L.?

La información por ser un activo valioso para las empresas, y depender de ella para el correcto funcionamiento, se requiere conservar su integridad, confidencialidad y disponibilidad por ser indispensable para el logro de los objetivos de la Cooperativa, motivo por el cual, necesitan colocar los medios para evitar robo y manipulación de sus datos confidenciales.

Los activos en las empresas sin importar su rubro requieren tanto de sus procesos y sistemas que permitan ser gestionados y protegidos convenientemente a partir de un análisis y tratamiento de riesgos, frente a las amenazas que puedan poner en peligro su integridad para alcanzar los objetivos, la seguridad de la Información no solamente es un problema de las grandes empresas sino de todo el mundo.

Justificación

1. **Contextualización y necesidad de seguridad de la información:** La cooperativa SIHUACOOP DE R.L., siendo pionera en el rubro y bien posicionada en El Salvador, se enfrenta a un entorno donde la seguridad de la información es cada vez más crucial. La falta de un sistema de gestión de la seguridad de la información expone a la cooperativa a diversos riesgos, tanto internos como externos. Es vital establecer un proceso adecuado para la gestión de la seguridad informática y la mitigación de riesgos.

2. **Cumplimiento normativo y mejores prácticas:** La norma ISO 27001 es reconocida a nivel internacional como el estándar de referencia para la gestión de la seguridad de la información. Adoptar esta norma permitirá a la cooperativa cumplir con los requerimientos y controles necesarios para establecer un Sistema de Gestión de Seguridad de la Información (SGSI). Al seguir las mejores prácticas y lineamientos de la norma, la cooperativa estará alineada con estándares reconocidos y aumentará su capacidad para enfrentar los desafíos en seguridad de la información. La norma ISO Ayudará al cumplimento de la normativa nacionales establecidas por la Superintendencia del Sistema Financiero (SSF) y el INSAFOCOOP.

3. **Protección de datos y confianza:** La implementación de un SGSI ayudará a gestionar eficientemente la accesibilidad de la información y garantizará la protección de los datos, información, procesos internos y detalles de pagos de la cooperativa. Esto es especialmente relevante considerando el crecimiento del uso y la importancia de los datos en la actualidad. Al implementar controles y procedimientos adecuados, la cooperativa demostrará su compromiso en fortalecer la seguridad de la información y generará confianza y credibilidad entre sus asociados.

4. **Mitigación de riesgos y cumplimiento de auditorías:** El SGSI propuesto en base a la norma ISO 27001 permitirá identificar y evaluar los riesgos de seguridad de la información, y definir pasos para su mitigación. Esto ayudará a prevenir incidentes de seguridad y a gestionarlos de manera adecuada en caso de que ocurran. Además, la implementación de la ISO 27001 asegurará que la cooperativa cumpla con el marco de las auditorías internas y externas, lo que fortalecerá la transparencia y la capacidad de respuesta de la cooperativa ante posibles riesgos y amenazas.

Objetivos

General

Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos, mitigar los riesgos de seguridad de la información y fortalecer la protección de los activos de información.

Específicos

- Evaluar el estado actual de la seguridad de la información en la cooperativa:
  - ✓ Realizar un análisis exhaustivo de los sistemas, procesos y controles de seguridad existentes en la cooperativa.
  - ✓ Identificar las vulnerabilidades, amenazas y riesgos de seguridad de la información a los que está expuesta la cooperativa.

- Diseñar un SGSI acorde a los requisitos de la norma ISO 27001:
  - ✓ Definir una metodología que sea aplicada a la cooperativa para el diseño de sistema de gestión de seguridad de la información.
  - ✓ Establecer un marco de gestión de riesgos que permita identificar, evaluar y tratar los riesgos de seguridad de la información de manera sistemática.
  - ✓ Establecer controles de seguridad adecuados para proteger los activos de información de la cooperativa.

Estado del arte

Fundamentación teórica

Los conceptos relacionados con la seguridad se aplican a cualquier tipo de organización, ya sea pública o privada, en el desarrollo de un sistema de gestión de seguridad de la información.

Sistema de Gestión de la Seguridad de la Información: SGSI es la sigla que se utiliza para hacer referencia a un Sistema de Gestión de la Seguridad de la Información, mientras que ISMS es su equivalente en inglés, que significa Information Security Management System. En este contexto, el término "información" hace referencia a cualquier conjunto de datos organizados que tenga valor para una entidad, independientemente de su forma de almacenamiento o transmisión (ya sea escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax, correo electrónico, transmitida en conversaciones, etc.), su origen (proveniente de la propia organización o de fuentes externas) o la fecha de creación.

Según ISO 27001, la seguridad de la información se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información y los sistemas utilizados en su tratamiento dentro de una organización. Estos tres términos son la base fundamental sobre la que se construye toda la estructura de seguridad de la información.

- *La confidencialidad* implica asegurar que la información sólo sea accesible por aquellos que tienen permiso para hacerlo.
- *La integridad* se refiere a la protección contra la alteración o modificación no autorizada de la información.
- *La disponibilidad* se refiere a la garantía de que la información esté disponible y sea accesible cuando se necesite.

La norma ISO 27001 establece un marco de referencia para la implementación de un SGSI, con el fin de asegurar la protección de la información y los sistemas que la procesan, así como la reducción de los riesgos relacionados con la seguridad de la información.

Norma ISO/IEC 27001:2022 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma proporciona un marco de trabajo para la gestión efectiva de la seguridad de la información en una organización, y su última revisión fue publicada en 2022.

La norma ISO 27001 se basa en la norma británica BS 7799-2 y puede ser implementada en cualquier tipo de organización, ya sea pública o privada, con o sin fines de lucro, pequeña o grande. La norma está redactada por expertos en seguridad de la información de todo el mundo, y proporciona una metodología para la implementación de un SGSI en una organización.

La implementación de la norma ISO 27001 permite a las organizaciones establecer un marco de gestión de la seguridad de la información, que se adapte a su estructura y necesidades. Además, la certificación ISO 27001 garantiza que una entidad independiente de certificación ha verificado que la organización ha implementado los requisitos de la norma en su SGSI, lo que aumenta la confianza de los clientes y partes interesadas en la seguridad de la información de la organización.

Análisis de Riesgo: es un proceso tanto cuantitativo como cualitativo que permite la evaluación de los riesgos. El primer paso en este proceso consiste en identificar los activos que se deben proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar.

Los resultados obtenidos del análisis permiten aplicar algunos de los métodos para el tratamiento de los riesgos. Estos métodos implican identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos. El análisis de riesgo involucra cinco elementos importantes que son: probabilidad, amenazas, vulnerabilidades, activos e impactos.

La probabilidad se refiere a la posibilidad de que ocurra un evento y se mide en términos de frecuencia. Las amenazas son eventos que pueden causar daño a un activo, mientras que las vulnerabilidades son debilidades que pueden ser explotadas por una amenaza. Los activos son los elementos de la organización que deben ser protegidos, y los impactos son las consecuencias que resultan de una amenaza que se materializa.

En resumen, el análisis de riesgo es un proceso crítico que permite identificar, evaluar y tratar los riesgos de seguridad de la información. Es un componente clave del sistema de gestión de seguridad de la información, y su aplicación puede ayudar a minimizar la exposición de una organización a riesgos innecesarios.

MAGERIT es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica. Su objetivo principal es estudiar los riesgos asociados a un sistema de información y su entorno, a través de la evaluación del impacto que una posible violación de la seguridad tendría en la organización. Para lograrlo, MAGERIT propone la realización de un análisis exhaustivo de los riesgos, que incluye la identificación de las amenazas que acechan al sistema de información y la determinación de la vulnerabilidad del sistema para prevenir dichas amenazas.

Una vez obtenidos los resultados del análisis, la gestión de riesgos puede recomendar las medidas apropiadas para prevenir, impedir, reducir o controlar los riesgos identificados, y así minimizar su potencialidad o sus posibles perjuicios. En definitiva, MAGERIT es una herramienta que permite a las organizaciones gestionar de manera eficiente y efectiva los riesgos asociados a la seguridad de la información.

CICLO DE MEJORA CONTINÚA EN LA NORMA ISO/IEC 27001:2022

Plan: Consiste en planificar acciones para hacer frente a los riesgos e identificar las oportunidades, para posteriormente evaluarlas y gestionarlas.

- Definir las políticas de seguridad de la información
- Establecer el alcance del SGSI
- Realizar el análisis de riesgo
- Seleccionar los controles de seguridad
- Definir competencias
- Establecer el mapa de riesgos
- Definir autoridades y responsabilidades

Hacer: Indica que la organización debe de disponer los recursos necesarios para establecer, implementar y mantener el SGSI, además de dar a conocer las políticas de seguridad de la información del SGSI.

- Poner en marcha el Plan de gestión de riesgos establecido
- Se implanta el SGSI
- Se establecen los controles de seguridad

Check – Controlar

- Revisar internamente el SGSI
- Realizar auditorias
- Se revisan los indicadores y métricas del SGSI

Actuar

- Realizan las acciones correctivas
- Realizan las acciones preventivas

Fundamentación legal

Descripción general:

El análisis del marco legal tiene como objetivo proporcionar un conocimiento general de la legislación cooperativa nacional y de sus principales características y contenidos, con especial atención a aquellos aspectos de la regulación relacionados con la identidad de las cooperativas y su distinción de otros tipos de organizaciones empresariales, en particular las con fines de lucro. corporación de accionistas.

Tiene como objetivo evaluar si la legislación nacional vigente apoya u obstaculiza el desarrollo de las cooperativas y, por lo tanto, es "favorable a las cooperativas" o no, y el grado en que puede considerarse así, también en comparación con la legislación vigente en otros países de la región de la ACI, o a nivel supranacional.

Además, la investigación tiene como objetivo brindar recomendaciones para una eventual renovación de los marcos legales vigentes con el fin de comprender qué cambios en la legislación actual serían necesarios para mejorar su grado de “favorabilidad cooperativa”, es decir, hacer que la legislación más favorable a las cooperativas, también en consideración a su identidad específica. Esta página web presenta una visión de los resultados del análisis del marco legal para El Salvador.

En El Salvador, la Constitución de la República promulgada en 1986, regula en su artículo 114 que: “El Estado protegerá y fomentará las Asociaciones Cooperativas, facilitando su organización, expansión y financiamiento”. De ahí su fundamento para la legislación secundaria que regula actualmente a las Asociaciones Cooperativas denominada “Ley General de Asociaciones Cooperativas “, promulgada por Decreto Legislativo número Trescientos treinta y nueve, de fecha seis de mayo de mil novecientos ochenta y seis, publicada en el Diario Oficial número ochenta y seis, tomo

doscientos noventa y uno de fecha catorce de mayo de ese mismo año, la cual vino a sustituir a la Ley de Cooperativas de 1969.

Favorabilidad cooperativa

Los aspectos tributarios de las cooperativas en El Salvador no difieren en cuanto a la naturaleza de los otros sujetos obligados a pagar impuestos, y las cooperativas están exentas únicamente de los impuestos sobre la renta y municipales. En cuanto a considerar si la ley es favorable o desfavorable al desarrollo de las cooperativas, se puede decir que es favorable porque se trata de una ley simple, no restrictiva, que puede tener una respuesta favorable a inquietudes no resueltas.

Leyes nacionales en El Salvador

- Ley Especial contra Delitos Informáticos y conexos en El Salvador.
- La Constitución de la Republica de El Salvador.
- Ley General de Asociaciones Cooperativas.
- Reglamento general de asociaciones cooperativas.
- Ley de Telecomunicaciones.
- Código Penal.
- Ley de Firma Electrónica.

Ley especial contra delitos informáticos y conexos en el salvador

La Ley Especial Contra Delitos Informáticos y Conexos fue aprobada en El Salvador el 14 de marzo de 2016 y entró en vigor el 13 de septiembre del mismo año., conocida también como "Ley de Cibercrimen", tiene como objetivo principal la protección de la seguridad informática y la privacidad de los datos de las personas, así como la prevención y sanción de los delitos informáticos que puedan causar daños o perjuicios a individuos o empresas.

La ley establece una serie de delitos informáticos, como la interceptación ilegal de datos, el acceso no autorizado a sistemas informáticos, el sabotaje informático, la difusión de virus informáticos, estafa informática, entre otros, establece penas y sanciones para aquellos que los cometan. También se proveen medidas para la protección de la información y la privacidad, como la obligación de los proveedores de servicios de

internet y los responsables de bases de datos de proteger la información de sus usuarios.

En nuestro país se carecía de una Ley como esta que a su vez también es el instrumento jurídico que vela por la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley.

Conocer esta ley y sensibilizar a los responsables del manejo de datos en las empresas públicas es de suma importancia ya que está en su Art. 2 cita que se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador. Los datos son y seguirán siendo un activo valioso y estratégico, siendo los líderes y titulares los principales protectores hoy más que nunca.

En conclusión, ley de delito informático en El Salvador busca proteger la seguridad y privacidad informática de las personas y empresas, prevenir y sancionar los delitos informáticos, y promover la seguridad en el uso de las tecnologías de la información y la comunicación en el país.

La Constitución de la República de El Salvador

La Asamblea Legislativa de la Republica de El Salvador, DECRETO Nº 38 Nosotros, representantes del pueblo salvadoreño reunidos en asamblea constituyente, puesta nuestra confianza en Dios, nuestra voluntad en los altos destinos de la patria y en ejercicio de la potestad soberana que el pueblo de El Salvador nos ha conferido, animados del ferviente deseo de establecer los fundamentos de la convivencia nacional con base en el respecto a la dignidad de la persona humana, en la construcción de una sociedad más justa, esencia de la democracia y al espíritu de libertad y justicia, valores de nuestra herencia humanista, decretamos, sancionamos y proclamamos, la siguiente: C O N S T I T U C I O N.

Ley General de Asociaciones Cooperativas

Este documento tiene como finalidad regular toda actividad relacionada con las necesidades del Movimiento Cooperativo Salvadoreño.

En el DECRETO Nº 339. LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR, CONSIDERA:

I. Que el Art. 114 de la Constitución establece que el Estado protegerá y fomentará las asociaciones cooperativas, facilitando su organización, expansión y financiamiento;

II. Que con base a la disposición constitucional antes citada y en atención al rápido crecimiento del movimiento cooperativo en el país y a la necesidad que tienen las asociaciones cooperativas de contar con una legislación adecuada y dinámica que responda a las necesidades del Movimiento Cooperativo Salvadoreño, que le permita desarrollarse social, económica y administrativamente, es conveniente dictar la legislación correspondiente;

POR TANTO, en uso de sus facultades constitucionales y a iniciativa del presidente de la República por medio de los ministros de Planificación y Coordinación del Desarrollo Económico y Social, Economía, Trabajo y Previsión Social y Agricultura y Ganadería y del Diputado Juan Bautista Ulloa, DECRETA la siguiente: LEY GENERAL DE ASOCIACIONES COOPERATIVAS TITULO I DE LAS ASOCIACIONES COOPERATIVAS

CAPITULO I De las Disposiciones Fundamentales Art. 1.- Se autoriza la formación de cooperativas como asociaciones de derecho privado de interés social, las cuales gozarán de libertad en su organización y funcionamiento de acuerdo con lo establecido en esta ley, la ley de creación del Instituto Salvadoreño de Fomento Cooperativo (INSAFOCOOP), sus Reglamentos y sus Estatutos.

Las Asociaciones Cooperativas de producción agropecuaria, pesquera y demás similares que desarrollen actividades técnicamente consideradas como agropecuarias, también se regirán de acuerdo con lo establecido en esta ley, en lo que no estuviere previsto en su Ley Especial. Las Cooperativas son de capital variable e ilimitado, de duración indefinida y de responsabilidad limitada con un número variable de miembros. Deben constituirse con propósitos de servicio, producción, distribución y participación.

Reglamento General de Asociaciones Cooperativas

Es un documento legislativo el Reglamento de la ley general de asociados de cooperativa.

En el DECRETO Nº 62. EL PRESIDENTE DE LA REPUBLICA DE EL SALVADOR.

CONSIDERANDO:

I. Que por Decreto Legislativo Nº 339, de fecha 6 de mayo de 1986, publicado en el Diario Oficial Nº 86, Tomo 291, del 14 de mayo del mismo año, se emitió la "LEY GENERAL DE ASOCIACIONES COOPERATIVAS", por medio de la cual se autoriza la formación de Cooperativas como asociaciones de derecho privado de interés social, las cuales gozarán de libertad en su organización y funcionamiento de conformidad con las leyes y sus Estatutos;
II. Que de conformidad con el Art. 99 de la referida Ley, el presidente de la República dictará dentro de los noventa días siguientes a la vigencia de la Ley, ¡el Reglamento de la misma;

POR TANTO: En uso de sus facultades constitucionales DECRETA: REGLAMENTO DE LA LEY GENERAL DE ASOCIACIONES COOPERATIVAS.

Ley de Telecomunicaciones en El Salvador

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR, DECRETA, la siguiente: LEY DE TELECOMUNICACIONES.

La presente Ley tiene por objeto normar, regular y supervisar las actividades relacionadas con el sector de las Telecomunicaciones y las Tecnologías de la información y la comunicación, que incluye la gestión del espectro radioeléctrico; el acceso a recursos esenciales; el plan de numeración, el servicio público de telefonía; la administración eficiente de las redes; la calidad, la cobertura y la continuidad de los servicios de telecomunicaciones y la protección de los derechos de los usuarios.

Concesión para el servicio público de telefonía.

La telefonía es un servicio público.

La SIGET determinará el valor máximo tanto de las tarifas básicas del servicio público de telefonía fija y móvil, como de los cargos básicos de interconexión, en ambos casos que vienen siendo ya regulados por SIGET. De la titularidad y la gestión del espectro radioeléctrico, el espectro radioeléctrico es un recurso natural limitado y es un bien demanial intangible, propiedad del estado.

La SIGET es la entidad estatal responsable de la gestión del espectro radioeléctrico. esta gestión abarca la planificación, administración, monitoreo y control técnico del uso y explotación del espectro radioeléctrico, de forma racional, eficiente, sostenible y equitativa, haciendo uso de los procedimientos y recursos que requiera

La SIGET para tal fin, siendo estos de tipo: económicos, financieros, jurídicos, científicos y técnicos.

La SIGET en su condición de gestor del espectro deberá realizar entre otras. El espectro radioeléctrico se clasifica en espectro de uso libre, de uso oficial y de uso regulado. Todos los operadores de sistemas de comunicación por satélite que transmitan desde el territorio nacional deberán cumplir con requisitos.

Los operadores de servicios de telecomunicaciones tendrán derecho a tender líneas aéreas o subterráneas en calles, plazas, parques, caminos y en otros bienes nacionales de uso público para los fines de instalar las redes necesarias para la prestación de los servicios,

Loa Recursos de telecomunicaciones. El propósito de la ley considera recursos esenciales a la interconexión a todos los niveles, la señalización, los datos de facturación entre otros.

La interconexión de redes será libremente negociada, excepto en lo referente al acceso a recursos esenciales. Por protección al usuario, derechos, obligaciones y prohibiciones.

En la ley de telecomunicaciones se tienen obligaciones, infracciones, sanciones y prohibiciones. De la desconexión del servicio, Los operadores podrán suspender la prestación de sus servicios sin aviso previo al usuario. Se detallan procedimientos y disposiciones en la ley de telecomunicaciones.

Código Penal

El decreto de la constituyente el 2 de marzo de 1880 y el 28 de febrero del cuerpo legislativo. Se declara ley de la república el código penal el cual está compuesto por 541 artículos.

El código penal, nos menciona las disposiciones generales sobre los delitos y faltas de, las personas responsables y las penas. Los delitos, faltas y las circunstancias que eximen de responsabilidad criminal, la atenúan o la agravan.

Las penas en general, de la clasificación de las penas como correccionales, leves, accesorias. De la duración y efecto de las penas. El efecto de las penas según su naturaleza respectiva. Tiene reglas para la aplicación de las penas en consideración a las circunstancias agravantes o atenuantes.

Delitos y faltas. Es delito o falta toda acción u omisión voluntaria penada por la ley. Garantías penales mínimas y aplicación de la ley penal. Hecho punible y responsabilidad penal. Penas. Medidas de seguridad. Extinción de la responsabilidad penal y sus efectos. Consecuencias civiles del hecho punible. Consecuencias accesorias. De los delitos y sus penas. Delitos relativos a la vida. Delitos relativos a la integridad personal. Delitos relativos a la libertad. Delitos contra la libertad sexual. Delitos relativos a la seguridad personal.

Delitos relativos al honor y la intimidad. Delitos relativos a las relaciones familiares. De los delitos relativos al patrimonio. Delitos relativos al orden socioeconómico. Delitos relativos a la ordenación del territorio, la protección de los recursos naturales y al medio ambiente. Delitos relativos a la seguridad colectiva. Delitos relativos a la salud pública. Delitos relativos a la fe pública. Delitos relativos a los derechos y garantías fundamentales de la persona. Delitos relativos a la administración de justicia. Delitos relativos a la administración pública. Delitos relativos al sistema constitucional y la paz pública. Delitos relativos a la existencia, seguridad y organización del Estado. Delitos contra la humanidad. Delitos de carácter internacional. Las faltas y sus penas.

Ley de Firma Electrónica

La Asamblea Legislativa de la Republica de El Salvador aprueba el DECRETO 133 de la Ley de firma electrónica.

En las disposiciones generales se maneja el objeto y alcance de la ley de firma electrónica, donde Equipara la firma electrónica simple y firma electrónica certificada con la firma autógrafa.

La presente ley maneja definiciones y principios generales entre las que podemos mencionar la Acreditación: Es la autorización que otorga la autoridad competente establecida en la presente Ley,

Firma Autógrafa: Marca o signo, que una persona escribe de su propia mano en un instrumento o documento para asegurar o autenticar la identidad de una persona, entre otras, y algunos principios son la autenticidad, integridad, confidencialidad, no repudiación. Se tienen reglas para el tratamiento de datos personales.

La equivalencia y valor jurídico de la firma electrónica, la firma electrónica simple tendrá la misma validez jurídica que la firma autógrafa.

Se maneja la emisión y recepción de los mensajes de datos y la firma electrónica certificada y certificados electrónicos, donde la firma electrónica certificada debe estar sustentada en un método de creación y verificación confiable y seguro, de manera que aquélla sea inalterable, alertando al destinatario en caso de modificación de la información.

El uso de la firma electrónica por los órganos de gobierno, donde se maneja el uso de una firma electrónica simple y el uso de una firma electrónica certificada, la validez de actas y contratos. Se tiene la autoridad competente, que están la autoridad de control y vigilancia, la unidad de forma electrónica.

Leyes o Normativas en La Cooperativa SIHUACOOP DE R.L.

Los Estatutos de La Cooperativa SIHUACOOP DE R.L.

Permiten guían el actuar de la Cooperativa y establecen tener claridad sobre la operación, el manejo y la forma de cumplir con las disposiciones legales.

Los estatutos de la Cooperativa son las normas internas que permiten tener claridad sobre la operación, el manejo y la forma de cumplir con las disposiciones legales. Incluye los siguientes aspectos:

- Razón social.
- Objeto del Acuerdo Cooperativo.
- Derechos y deberes de los asociados.
- Régimen de sanciones, causales y procedimientos.
- Régimen de organización interna.
- Régimen y responsabilidad de la Cooperativa y de sus asociados.
- Normas para fusión, incorporación, transformación, disolución y liquidación.
- Aportes sociales mínimos no reducibles durante la vida de la Cooperativa, forma de pago y devolución.

Los Reglamentos e Instructivos de La Cooperativa SIHUACOOP DE R.L.

Según DECRETO Nº 62. EL PRESIDENTE DE LA REPUBLICA DE EL SALVADOR. CONSIDERANDO:

I. Que por Decreto Legislativo Nº 339, de fecha 6 de mayo de 1986, publicado en el Diario Oficial Nº 86, ¡Tomo 291, del 14 de mayo del mismo año, se emitió la LEY GENERAL DE ASOCIACIONES COOPERATIVAS, por medio de la cual se autoriza la formación de Cooperativas como asociaciones de derecho privado de interés social, las cuales gozarán de libertad en su organización y funcionamiento de conformidad con las leyes y sus Estatutos;

II. Que de conformidad con el Art. 99 de la referida Ley, el Presidente de la República dictará dentro de los noventa días siguientes a la vigencia de la Ley, el Reglamento de

la misma; POR TANTO: En uso de sus facultades constitucionales DECRETA: REGLAMENTO DE LA LEY GENERAL DE ASOCIACIONES COOPERATIVAS.

Capítulo II: Marco de trabajo

Alcance y Limitaciones

Alcances

- ✓ Se realizará el Diseño del Sistema de Gestión de Seguridad de la Información (SGSI): Se llevará a cabo el diseño del SGSI basado en la norma ISO 27001 para la Cooperativa SIHUACOOP DE R.L. Esto incluirá la definición de la estructura organizativa, roles y responsabilidades, así como la documentación de políticas y procedimientos de seguridad.
- ✓ Se incluirá la Identificación, valoración y clasificación de activos de información: Se realizará un proceso para identificar los activos de información críticos de la Cooperativa SIHUACOOP DE R.L. Esto implicará la categorización de los activos en términos de su importancia y su valor para la organización.
- ✓ Se realizará Análisis y evaluación de riesgos: Se llevará a cabo un análisis de riesgos para identificar las amenazas y vulnerabilidades que podrían afectar la seguridad de la información de la cooperativa. Se evaluará la probabilidad de ocurrencia y el impacto potencial de cada riesgo identificado.
- ✓ Se presentará un informe de resultados y recomendaciones: Una vez completado el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para la Cooperativa SIHUACOOP DE R.L., se elaborará un informe detallado que incluya los hallazgos principales de la investigación y evaluación realizadas. Este informe proporcionará una visión general de la situación actual de la seguridad de la información en la cooperativa, destacando los riesgos identificados y los controles propuestos para mitigarlos.

Limitaciones

- ✓ No se incluye la implementación del Sistema de Gestión de Seguridad de la Información (SGSI): Se centrará únicamente en el diseño del SGSI basado en la norma ISO 27001 para la Cooperativa SIHUACOOP DE R.L. Sin embargo, la implementación efectiva del SGSI requerirá recursos adicionales y una planificación detallada que excede el alcance de este trabajo.
- ✓ No se realizará el mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información: La fase de mantenimiento y revisión continua del SGSI, que implica la evaluación periódica de los controles de seguridad, la actualización de políticas y procedimientos, y la mejora continua, no será abordada en este trabajo y quedarían en entera responsabilidad de la Cooperativa.
- ✓ No se incluye capacitación sobre seguridad de la información: Aunque se mencionó la importancia de la concientización y capacitación del personal en las mejores prácticas de seguridad de la información, esta capacitación no será realizada como parte de este trabajo de grado. La capacitación requeriría una planificación y ejecución adicional para asegurar la comprensión y adopción adecuada de los controles de seguridad por parte de los empleados de la cooperativa.
- ✓ Recursos limitados: La cooperativa SIHUACOOP DE R.L. puede tener recursos limitados, como tiempo, personal y presupuesto. Estas limitaciones pueden dificultar la adquisición de herramientas y tecnologías necesarias, así como la implementación y mantenimiento de las medidas de seguridad.
- ✓ Conocimientos técnicos limitados: Es posible que la cooperativa carezca de personal con conocimientos especializados en seguridad de la información y la norma ISO 27001. Esto puede afectar la implementación efectiva de los controles y prácticas de seguridad requeridos, así como la toma de decisiones informadas y la identificación de áreas de mejora.
- ✓ Resistencia al cambio: Algunos miembros de la cooperativa podrían mostrar resistencia al cambio y ser reacios a adoptar nuevas prácticas y controles de seguridad de la información. Esta resistencia puede dificultar la implementación y la adopción de las medidas de seguridad necesarias.
- ✓ Limitaciones legales y regulatorias: Es importante tener en cuenta las leyes y regulaciones locales aplicables; puede haber restricciones legales o requisitos específicos que deban ser considerados durante el proceso de implementación.

Metodologías

Metodología de investigación

A fin de lograr los objetivos propuestos y contar con información que permita servir como documentación de los procesos a seguir, se incluirán las actividades propuestas por la norma ISO/IEC 27001:2022.

El proyecto de grado corresponde al análisis y diseño del sistema de gestión y seguridad de la información para la Cooperativa SIHUACOOP DE R.L. propuesto por la ISO 27001:2022 como guía base para la implementación, dicho diseño contempla el diagnóstico y análisis inicial de buenas prácticas de seguridad de la información basado en el estándar ISO/IEC 27001 revisión 2022, análisis y construcción de artefactos necesarios para la planeación del SGSI.

La metodología que ejecutaremos consiste en entrevistas no estructuradas con el Gerente de Tecnología de la cooperativa, visita a las instalaciones de la cooperativa con el fin de obtener un acercamiento y comprender su cultura organizacional, contexto de la organización, procesos de la cooperativa, la complejidad de estos y los problemas actuales.

Realizaremos una investigación descriptiva, donde se expondrá la situación actual del estado de la cooperativa respecto al sistema de gestión ISO 27001:2022.

La investigación descriptiva tiene como finalidad definir, clasificar, catalogar o caracterizar el objeto de estudio. Los métodos descriptivos pueden ser cualitativos o cuantitativos. Los principales métodos de la investigación descriptiva son observacionales, el de encuestas y los estudios de caso único.

Debido a que la naturaleza del proyecto de diseño de un sistema de gestión de seguridad de la información se ubica en la línea de investigación de gestión de la calidad. El proyecto se llevará a cabo explorando las fuentes primarias de información como entrevistas a los responsables de tecnología y secundaria como archivos, auditorias, análisis e información documentada que disponga la cooperativa. La identificación y correlación de los requisitos aplicables al sistema de gestión ISO 27001.

Metodología para establecer el SGSI

Para establecer un SGSI aplicado a la cooperativa lo segmentaremos en varias fases:

Fase 1: Análisis de necesidades

- Realizar un análisis exhaustivo de las necesidades específicas de seguridad de la información de la cooperativa.
- Identificar los activos de información críticos y los requisitos de seguridad asociados.
- Evaluar las amenazas y vulnerabilidades a las que se enfrenta la cooperativa en relación con la seguridad de la información.

Fase 2: Evaluación de cumplimiento actual

- Evaluar el estado de cumplimiento de los controles de seguridad existentes en la cooperativa, según los lineamientos y requisitos de la norma ISO 27001 en el anexo A, dominio y controles.
- Identificar las brechas y áreas de mejora en el cumplimiento de los controles de seguridad.

Fase 3: Análisis de riesgos

- Recopilar y analizar los riesgos a los que se expone la cooperativa debido a la falta de un SGSI.
- Evaluar el impacto y la criticidad de los riesgos identificados.
- Utilizar la metodología de la guía 27001, basada en la gestión de riesgos de la información, teniendo en cuenta los activos de la cooperativa.
- Obtener un diagnóstico detallado del estado actual de la cooperativa en términos de seguridad de la información.

Fase 4: Documentación del SGSI

- Documentar los procesos, formatos y metodologías necesarios para garantizar la seguridad de la información de acuerdo con las buenas prácticas y los requisitos de la norma ISO 27001.
- Elaborar un documento estructurado que contenga los requisitos sugeridos por la norma y sus guías para el diseño y la implementación del SGSI en la cooperativa.
- Asegurarse de que la documentación sea clara, completa y coherente con los objetivos y necesidades de seguridad de la cooperativa.

Metodología para el Análisis y Evaluación de Riesgos

Existen diferentes metodologías para gestionar el proceso de análisis, evaluación y gestión de riesgos informáticos, cada una con características propias y destinadas a situaciones y objetivos en particular.

Sin embargo, cada una de estas metodologías cuenta con actividades y componentes en común como son:

- **Identificación de amenazas:** Se enfoca en identificar las posibles amenazas a la seguridad de la información. Estas amenazas son los eventos y acciones que podrían alterar o perjudicar los activos relacionados a la seguridad de la información de la organización.
- **Identificación de vulnerabilidades:** Se enfoca en identificar las posibles vulnerabilidades que podrían ser explotadas por las amenazas previamente identificadas. Asimismo, la existencia de una vulnerabilidad contribuye a calcular la probabilidad del riesgo.
- **Identificación de activos:** Es el proceso en el cual se identifican los activos esenciales o críticos que tienen un impacto directo en la confidencialidad, integridad y disponibilidad de las fuentes de información de la organización.
- **Determinación del impacto:** Es el proceso para determinar o medir el impacto de una amenaza sobre un activo. Este impacto puede ser catalogado de forma cuantitativa o cualitativa.
- **Determinación de la probabilidad:** Esta actividad tiene como objetivo medir la probabilidad de ocurrencia de una determinada amenaza, para lo cual se le asigna un valor probable.
- **Identificación de controles:** Los controles permiten detectar o prevenir las fuentes de amenazas que tratan de explotar las vulnerabilidades. En esta actividad se identifican los controles que se están llevando a cabo sobre un activo y el efecto que tendría sobre la amenaza que se evalúa.

Metodología para el Tratamiento de Riesgos

La gestión de riesgos es un componente fundamental en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001. La metodología utilizada para el tratamiento de riesgos debe garantizar una gestión efectiva y homogénea en todas las áreas de la cooperativa SIHUACOOP DE R.L. Los siguientes pasos se seguirán en la metodología propuesta:

1. **Definición de la metodología y objetivo:**
   - Se definirá una metodología clara y comprensible para la gestión de riesgos, asegurando su aplicación consistente en toda la cooperativa.
   - El objetivo del proceso de gestión de riesgos será establecido, con el propósito de garantizar la continuidad del negocio y proteger la información sensible de la cooperativa.
2. **Evaluación cualitativa o cuantitativa de riesgos:**
   - Se definirá si la evaluación de riesgos se realizará de manera cualitativa o cuantitativa.
   - En el caso de la evaluación cualitativa, se establecerá una escala para definir y clasificar los niveles de riesgo como aceptables o no aceptables.
3. **Plan de gestión de riesgos:**
   - Se desarrollará un plan de gestión de riesgos que asegure la continuidad del negocio y la seguridad de la información.
   - El plan incluirá un análisis de riesgos de seguridad de la información en la cooperativa, abarcando el diseño, identificación y evaluación de la situación actual de los activos, así como la medición de los riesgos existentes.
4. **Clasificación y medición de riesgos:**
   - Los riesgos identificados serán clasificados en categorías, como desastres ambientales, procesos inadecuados de tratamiento de la información, desconocimiento de normas y políticas de seguridad, y falta de cumplimiento de las políticas de seguridad.
   - Se llevará a cabo la medición de los riesgos identificados y se propondrán medidas para reducirlos.
   - Se documentarán los tratamientos de riesgos estructurados y documentados para la cooperativa.
5. **Análisis detallado de riesgos:**
   - Se realizarán análisis detallados de los problemas que podrían surgir en la cooperativa, teniendo en cuenta los riesgos identificados.

- Se evaluarán y contabilizarán los activos de la cooperativa, indicando las amenazas y debilidades a las que podrían enfrentarse.
- Se establecerá la probabilidad de que cada riesgo ocurra.

Es importante documentar claramente la metodología utilizada, así como utilizar técnicas y herramientas apropiadas, como análisis de riesgos, evaluación cualitativa y cuantitativa, y matrices de riesgos. Además, será de gran importancia adaptar la metodología a las necesidades específicas de la cooperativa SIHUACOOP DE R.L. y cumplir con los requisitos establecidos en la norma ISO 27001.

Normas Internacionales en la familia de la ISO27001:2022

Familia de Normativas de la Serie ISO 27000

La norma da una perspectiva sobre la importancia del SGSI, el alcance de sus procesos y del establecimiento, monitoreo, mantenimiento y mejora del SGSI.

Asimismo, nos brinda una relación de la familia de estándares que acompañan a la normativa, los cuales son los siguientes:

ISO / IEC 27000, Sistemas de gestión de la seguridad de la información - Generalidades y vocabulario.

ISO / IEC 27001, Sistemas de gestión de la seguridad de la información - Requisitos.

ISO / IEC 27002, Código de prácticas para controles de seguridad de la información.

ISO / IEC 27003, Guía de implementación del sistema de gestión de seguridad de la información.

ISO / IEC 27004, gestión de seguridad de la información - Medición.

ISO / IEC 27005, gestión del riesgo de seguridad de la información.

ISO / IEC 27006, Requisitos para los organismos que proporcionan auditoría y certificación de la seguridad de la información sistemas de gestión.

ISO / IEC 27007, Directrices para la auditoría de sistemas de gestión de la seguridad de la información.

ISO / IEC TR 27008, Directrices para auditores sobre controles de seguridad de la información.

ISO / IEC 27009, Aplicación sectorial de ISO / IEC 27001 – Requisitos.

ISO / IEC 27010, gestión de la seguridad de la información para las comunicaciones intersectoriales e interorganizacionales.

ISO / IEC 27011, Directrices de gestión de seguridad de la información para organizaciones de telecomunicaciones basado en ISO / IEC 27002.

ISO / IEC 27013, Orientación sobre la implementación integrada de ISO / IEC 27001 e ISO / IEC 20000-1

ISO / IEC 27014, Gobernanza de la seguridad de la información.

ISO / IEC TR 27015, Directrices de gestión de seguridad de la información para servicios financieros.

ISO / IEC TR 27016, gestión de seguridad de la información - Economía organizacional.

ISO / IEC 27017, Código de prácticas para controles de seguridad de la información basado en ISO / IEC 27002 para servicios de la nube.

ISO / IEC 27018, Código de prácticas para la protección de la información de identificación personal pública en la nube.

ISO / IEC 27019, Directrices de gestión de la seguridad de la información basadas en ISO / IEC 27002 para el proceso sistemas de control específicos para la industria de servicios energéticos.

ISO 27799, Informática de salud - Gestión de la seguridad de la información en salud utilizando ISO / IEC 27002

Entidades que normalizan o certifican la Seguridad Informática

En El Salvador, no hay un organismo específico encargado de velar por el cumplimiento de la norma ISO 27001.

Sin embargo, existen organizaciones que ofrecen servicios de consultoría y certificación en ISO 27001, como firmas de consultoría y empresas de certificación reconocidas internacionalmente, como:

- Bureau Veritas
- TÜV Rheinland
- DNV,
- ICONTEC
- ENAC
- DQSGLOBAL
- DELOITTE
- entre otras

Las empresas mencionadas pueden ayudar a las organizaciones a implementar y cumplir con los requisitos de la norma ISO 27001 y obtener la certificación

Instituciones que regulan a las Cooperativas

El Instituto Salvadoreño de Fomento Cooperativo - INSAFOCOOP

El Cooperativismo es asociativo, nace para defender a las personas, surgen las asociaciones en forma de empresa propia destinada a satisfacer las necesidades comunes de las mismas. El Cooperativismo en materia socio económica defiende a las personas, en su doble carácter “como consumidores y productores”. Los considerados padres del cooperativismo moderno son Roben Owen y Willian King, pero también contribuyeron grandemente otros pensadores franceses y alemanes. En El Salvador se escucha, por primera vez, del cooperativismo en forma teórica, en una cátedra de enseñanza, en la facultad de jurisprudencia y ciencias sociales de la Universidad de El Salvador. Fue en 1914, que se organiza la primera cooperativa, por un grupo de zapateros, en San Salvador en la cuesta del Palo Verde y en 1938, se funda la Cooperativa Algodonera.

Luego el Cooperativismo llego al gremio de los empleados públicos, como un medio de defensa contra el agiotismo. Las cooperativas contaban con el apoyo del gobierno en turno, que aportaba capital inicial, pero los empleados identificaban el capital cedido por el gobierno, como propiedad de ellos y no creyeron que estuvieran obligados, por esa razón, a resarcir las cantidades que se les concedían en calidad de préstamo. Así mismo el surgimiento de secciones y departamentos en instituciones gubernamentales el sector inició su crecimiento hasta que el Estado decide centralizar este rol en una sola Institución que dirija y coordine la actividad cooperativa en el país. Fue el 25 de noviembre de 1969 que la Asamblea Legislativa, promulgó el Decreto No. 560 que dio pie a la creación del **INSAFOCOOP** como una corporación de derecho público con autonomía en los aspectos económico y administrativo, ese mismo día se promulga la primera Ley General de Asociaciones Cooperativas. A falta de presupuesto que permitiera su funcionamiento el INSAFOCOOP comenzó a operar hasta el 1 de julio de 1971.

Comisión Financiera de La Asamblea Legislativa

La Comisión Financiera, no es una institución que regula a las cooperativas, pero es una comisión creada por el poder legislativo. Se creó con el fin de adecuar, revisar y legislar, los diferentes temas del ámbito financiero de El Salvador, que son de mucha preocupación e importancia para la Economía del País; por el impulso de la globalización específicamente en la reintegración de los circuitos económicos mundiales de los países de tercer y cuarto mundo, con el fin de encontrar soluciones eficaces que minimicen el impacto de la Economía en los salvadoreños.

La Comisión Financiera estudia regulación de cooperativas y asociaciones para evitar prácticas abusivas en todo El Salvador.

Legislación Informática de República de El Salvador - Leyes y Decretos

Ley de 22 de abril de 2021. Ley de Protección de Datos Personales y Habeas Data.

Ley de 22 de abril de 2021. Ley de Creación de la Autoridad Nacional Digital.

Decreto 100 de 20 de julio de 2021, que modifica varios artículos de la Ley de Firma Electrónica

Decreto nº 133, de 1 de octubre de 2015. Aprobación de la Ley de Firma Electrónica. (Diario Oficial número 196, tomo nº 409, de 26 de octubre de 2015).

Decreto nº 260, de 4 de febrero de 2016. Ley Especial contra los Delitos Informáticos y Conexos. (Diario Oficial número 40, tomo nº 410, de 26 de febrero de 2016).

Decreto nº 136, de 1 de septiembre de 2011. Reglamento de la Ley de Acceso a la Información Pública (Diario Oficial número 163, tomo nº 392, del 2 de septiembre de 2011)

Decreto nº 534, de 2 de diciembre de 2010. Ley de Acceso a la Información Pública. (Diario Oficial número 70, tomo nº 371, de 8 de abril de 2011).

Decreto nº 695, de 29 de abril de 2011. Ley de Regulación de los Servicios de Información sobre el historial de crédito de las personas. (Diario Oficial número 141, tomo nº 392, de 27 de julio de 2011).

Decreto nº 697 de 27, de septiembre de 1999, que regula el servicio información crediticia y Secreto Bancario.

Decreto nº 697 de 27, de septiembre de 1999, que regula el servicio información crediticia y Secreto Bancario.

Cronograma

Ilustración 2. Cronograma Duración Programada

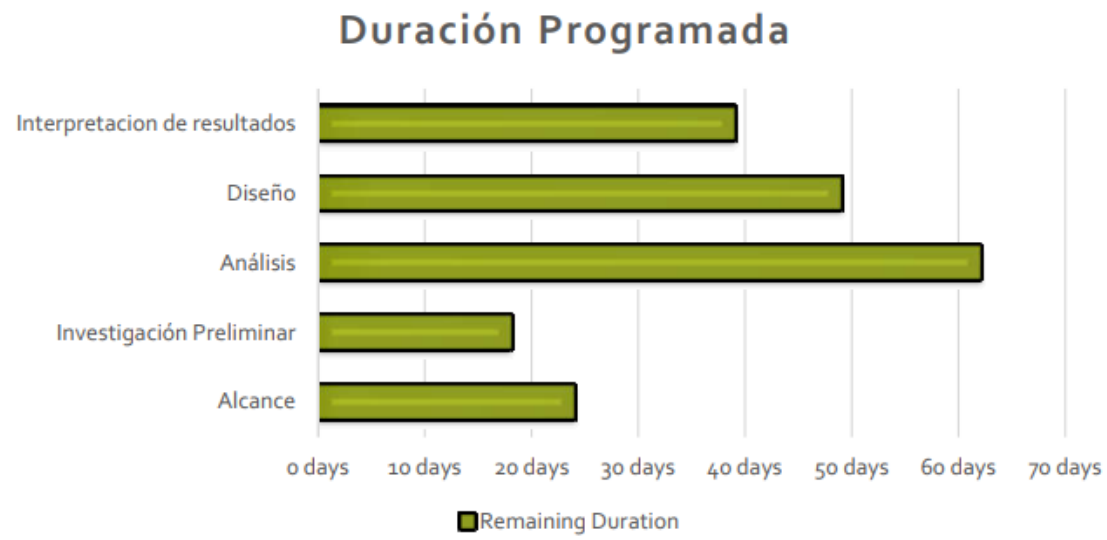
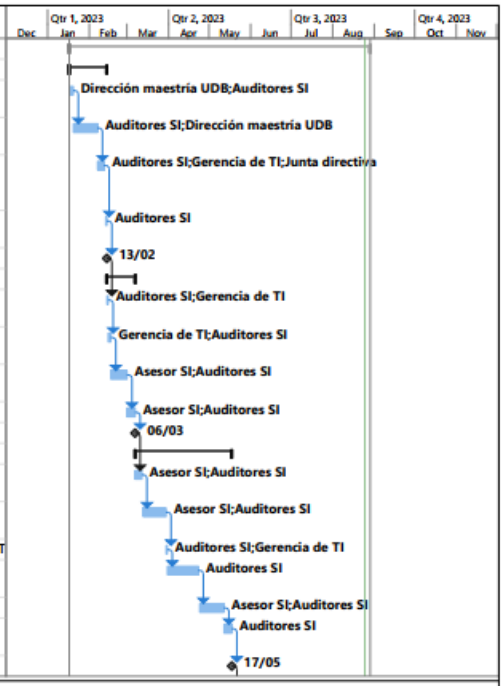


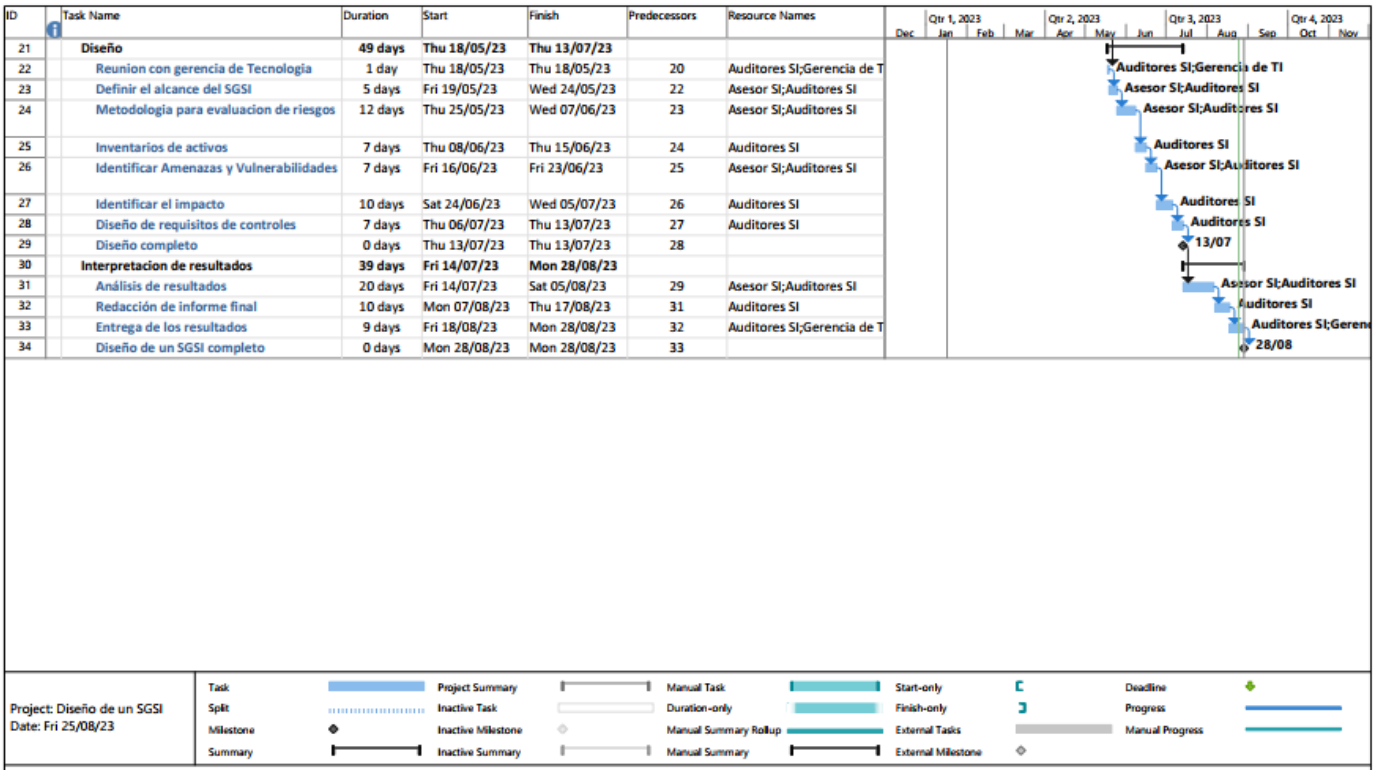
Tabla 3. Detalle Cronograma Duración Programada

ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
0	**Diseño de un SGSI**	**192 days**	**Tue 17/01/23**	**Mon 28/08/23**		
1	**Alcance**	**24 days**	**Tue 17/01/23**	**Mon 13/02/23**		
2	Delimitación del Problema de investigación o Trabajo de Aplicación.	3 days	Tue 17/01/23	Thu 19/01/23		Dirección maestría UDB;Auditores SI
3	Realizar el Perfil de Trabajo de Graduación.	15 days	Fri 20/01/23	Mon 06/02/23	2	Auditores SI;Dirección maestría UDB
4	Elaborar de solicitud para realizar trabajo de Graduacion en Cooperativa.	5 days	Tue 07/02/23	Sat 11/02/23	3	Auditores SI;Gerencia de TI;Junta directiva
5	Establecer un Calendario de actividades.	1 day	Mon 13/02/23	Mon 13/02/23	4	Auditores SI
6	Alcance completo.	0 days	Mon 13/02/23	Mon 13/02/23	5	
7	**Investigación Preliminar**	**18 days**	**Tue 14/02/23**	**Mon 06/03/23**		
8	Visita de reconocimiento de las instalaciones de la cooperativa.	1 day	Tue 14/02/23	Tue 14/02/23	6	Auditores SI;Gerencia de TI
9	Recolección de la Información del negocio.	2 days	Wed 15/02/23	Thu 16/02/23	8	Gerencia de TI;Auditores SI
10	Analisis de la informacion compartida por la cooperativa.	10 days	Fri 17/02/23	Tue 28/02/23	9	Asesor SI;Auditores SI
11	Revision de reportes anteriores.	5 days	Wed 01/03/23	Mon 06/03/23	10	Asesor SI;Auditores SI
12	Investigación completo	0 days	Mon 06/03/23	Mon 06/03/23	11	
13	**Análisis**	**62 days**	**Tue 07/03/23**	**Wed 17/05/23**		
14	Definición y desarrollo de herramientas y metodología	5 days	Tue 07/03/23	Sat 11/03/23	12	Asesor SI;Auditores SI
15	Realizar anteProyecto de Trabajo de Graduación	15 days	Mon 13/03/23	Wed 29/03/23	14	Asesor SI;Auditores SI
16	Reunion con gerencia de Tecnologia	1 day	Thu 30/03/23	Thu 30/03/23	15	Auditores SI;Gerencia de T
17	Identificación de los recursos humanos y tecnológicos.	20 days	Fri 31/03/23	Sat 22/04/23	16	Auditores SI
18	Realizar evaluación de riesgos.	16 days	Mon 24/04/23	Thu 11/05/23	17	Asesor SI;Auditores SI
19	Identificación de los requisitos de cumplimiento	5 days	Fri 12/05/23	Wed 17/05/23	18	Auditores SI
20	Análisis completo	0 days	Wed 17/05/23	Wed 17/05/23	19	



Project: Diseño de un SGSI
Date: Fri 25/08/23

Task | Split | Milestone | Summary | Project Summary | Inactive Task | Inactive Milestone | Inactive Summary | Manual Task | Duration-only | Manual Summary Rollup | Manual Summary | Start-only | Finish-only | External Tasks | External Milestone | Deadline | Progress | Manual Progress



ID	Task Name	Duration	Start	Finish	Predecessors	Resource Names
21	**Diseño**	**49 days**	**Thu 18/05/23**	**Thu 13/07/23**		
22	Reunion con gerencia de Tecnologia	1 day	Thu 18/05/23	Thu 18/05/23	20	Auditores SI;Gerencia de T
23	Definir el alcance del SGSI	5 days	Fri 19/05/23	Wed 24/05/23	22	Asesor SI;Auditores SI
24	Metodologia para evaluacion de riesgos	12 days	Thu 25/05/23	Wed 07/06/23	23	Asesor SI;Auditores SI
25	Inventarios de activos	7 days	Thu 08/06/23	Thu 15/06/23	24	Auditores SI
26	Identificar Amenazas y Vulnerabilidades	7 days	Fri 16/06/23	Fri 23/06/23	25	Asesor SI;Auditores SI
27	Identificar el impacto	10 days	Sat 24/06/23	Wed 05/07/23	26	Auditores SI
28	Diseño de requisitos de controles	7 days	Thu 06/07/23	Thu 13/07/23	27	Auditores SI
29	Diseño completo	0 days	Thu 13/07/23	Thu 13/07/23	28	
30	**Interpretacion de resultados**	**39 days**	**Fri 14/07/23**	**Mon 28/08/23**		
31	Análisis de resultados	20 days	Fri 14/07/23	Sat 05/08/23	29	Asesor SI;Auditores SI
32	Redacción de informe final	10 days	Mon 07/08/23	Thu 17/08/23	31	Auditores SI
33	Entrega de los resultados	9 days	Fri 18/08/23	Mon 28/08/23	32	Auditores SI;Gerencia de T
34	Diseño de un SGSI completo	0 days	Mon 28/08/23	Mon 28/08/23	33	

Capítulo III: Análisis y Diseño de SGSI

Definición de herramientas y Metodología utilizada para la gestión de riesgo.

Un Sistema de Gestión de Seguridad Informática (SGSI) se encuentra determinada por la estructura organizacional de las instituciones, lo que abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001, norma en la que se describen un conjunto de herramientas corporativas que permiten establecer un plan de acción para la solución de problemas de seguridad a nivel técnico, organizativo y legislativo en una empresa. Estos sistemas utilizan como requisitos, estrategias como el análisis, evaluación y gestión de riesgos dentro del ciclo de Deming que es un sistema que busca perfeccionar u optimizar permanentemente las operaciones empresariales mediante 4 etapas. En español, se conoce como el ciclo PDCA (Planificar, Hacer, Verificar y Actuar).

Ilustración 3. Ciclo PDCA ISO/IEC 27001

Procesos SGSI dentro del Ciclo Deming, nosotros nos enfocaremos precisamente en los procesos definidos dentro de la etapa de planificar, como se muestra en la ilustración siguiente:

Ilustración 4. Relación Ciclo de Deming con Procesos SGSI

CICLO DEMING	PROCESOS SGSI
Planificar	Definir alcance del SGSI. Definir política de seguridad. Metodología de evaluación de riesgos. Inventario de activos. Identificar amenazas y vulnerabilidades. Análisis y evaluación de riesgos. Selección de controles.
Hacer	Definir plan de tratamiento de riesgos. Implantar plan de tratamiento de riesgos. Implementar los controles. Formación y concienciación. Operar el SGSI.
Verificar	Revisar el SGSI. Medicar eficacia de los controles. Revisar riesgos residuales. Realizar auditorías internas del SGSI. Realizar acciones y eventos.
Actuar	Implantar mejoras. Acciones correctivas y preventivas. Comprobar eficacia de las acciones.

Esta selección requiere una metodología sistemática que permita obtener una visión clara y priorizada de los riesgos a los que se enfrenta la organización, identificando los más relevantes y priorizando medidas para minimizar la probabilidad de materialización de dichos riesgos o el impacto, en caso de materializarse.

Metodología Aplicada

Estableceremos una metodología de análisis de riesgos dentro de los SGSI, lo que permitirá dar a conocer las debilidades y fortalezas con que cuenta una organización por cada uno de sus activos informáticos; se logrará identificar y valorar los procesos más críticos del negocio, con el propósito de evaluar el nivel de protección adecuado, determinar y evaluar las amenazas y su grado de efectividad para hacer frente a los riesgos y calcular el nivel de los mismos, de tal forma, que la organización conozca con detalle la probabilidad de materialización de cada una de las amenazas.

Para ello hemos definido como método de análisis y gestión de riesgo a MAGERIT que es una metodología elaborada por el Consejo Superior de Administración Electrónica de España, que busca gestionar de una forma sistemática los riesgos a los que se puede

ver expuestos las diferentes organizaciones en temas relacionados a la seguridad informática. Esta metodología define objetivos claros trazables y alcanzables para las organizaciones y permite realizar un seguimiento exhaustivo del avance de estos.

Técnica

Utilizaremos la técnica de análisis de riesgo propuesta por Instituto de Ciberseguridad de España - “INCIBE”, que nos van a facilitar el análisis de riesgos y vulnerabilidades la cual recoge las principales amenazas a considerar en el ámbito de un análisis de riesgos. Se trata de un extracto ligeramente modificado del catálogo de amenazas de MAGERIT Versión 3, esta se basa en una escala de probabilidad e impacto de tres niveles.

Con esta técnica se determinarán los siguientes puntos:

1. Determinar el riesgo aceptable.
2. Identificar los activos críticos de la organización
3. Identificar las amenazas que aplican a cada uno de los activos críticos.
4. Establecer la probabilidad y el impacto de que dicha amenaza se materialice.
5. Establecer medidas para aquellos riesgos que superen el riesgo aceptable indicado.

Identificación de recursos humanos y tecnológicos

Fundamentos.

La política de la cooperativa se identifica comúnmente como formalidades de normas de conducta que se aplican dentro de la entidad.

Al delimitar la manera de actuar del personal de acuerdo con lo que se espera en áreas donde puede ser necesario definir mejor el contexto del trabajo de la cooperativa.

De acuerdo con lo señalado por el numeral A5.2 del estándar la ISO 27001 que nos menciona las funciones y responsabilidades de la seguridad de la información, se determinará un marco general dentro del cual serán proporcionados la seguridad de la información y los objetivos generales para garantizar la continuidad del negocio a fin de limitar o prevenir el daño potencial a los activos de la cooperativa a un nivel aceptable y, limitar las posibles consecuencias de incidentes de seguridad.

Entre los activos de la cooperativa SIHUACOOP que se pueden mencionar se tienen los siguientes:

- Hardware (servidores informáticos, equipos de red, ordenadores, portátiles, impresores, UPS, etc.);
- Software (licenciamiento en sistemas operativos, ofimática, aplicaciones y Core financiero);
- Información (registros en papel y digitales);
- Personas (empleados, contratistas, voluntarios y cualquier persona que conozca información confidencial);
- Servicios (prestados por la cooperativa que es ahorro y crédito); y
- Las ubicaciones.

La Estructura Organizacional del SGSI para la Cooperativa SIHUACOOP

En la ISO 27001:2022, en la sección de los controles de la organización A.5 se indica en el numeral A5.1 política de seguridad de la información, la participación activa y el compromiso que tenga la gerencia de la cooperativa en el SGSI es esencial para desarrollar y mantener un SGSI efectivo. La dirección ayuda a crear una cultura de seguridad de la información y educar a todos los miembros de la organización. La administración debe aprobar el proyecto del Plan de SGSI.

En la cooperativa no se había considerado anteriormente el hecho de contar con una persona que sea el responsable de la seguridad de la información, pues evaluaba que al área de Informática podían controlar las funciones y acciones relevantes a la seguridad.

Estructura Organizativa con la que se cuenta actualmente
en el Departamento de Tecnología De la Cooperativa SIHUACOOP DE R.L.

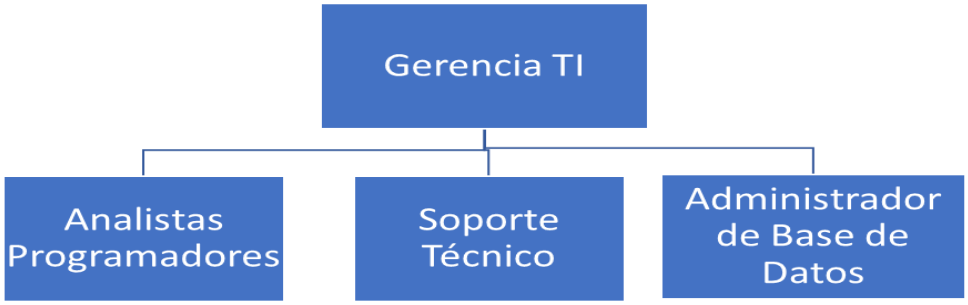


Ilustración 5. Organigrama TI Actual. Elaboración por la Cooperativa SIHUACOOP DE R.L.

Algunas debilidades que se han encontrado con la estructura organizativa podemos mencionar las siguientes:

- Falta un especialista que pueda realizar las funciones de infraestructura para separar funciones y haya mejor dedicación a los puestos de trabajo en el departamento de tecnología.
- Segregar funciones y responsabilidades a cada puesto de trabajo, para que el personal de tecnología se dedique a sus tareas y no todo el personal hagan lo mismo.

La estructura que se menciona a continuación hace énfasis a lo mínimo necesario que pudiera tener el departamento de tecnología de la Cooperativa SIHUACOOP.

Se puede mencionar que, con la estructura logrará que todas las áreas dentro del departamento de tecnología puedan ser atendidas por un especialista con funciones y responsabilidades bien específicas para lograr los objetivos y metas planificadas, de tal forma que se puedan obtener mejores resultados.

La siguiente estructura organizativa es una propuesta para el departamento de tecnología, con la finalidad que se pueda lograr en un periodo a largo plazo dentro de una planificación estratégica, la cual tendría una visión, una misión y objetivos hacia donde quiere llegar, se podrían agregar más puestos de trabajo, pero dependerá de la situación en la que se encuentre la cooperativa y de la demanda que se pueda llegar a tener en servicios con tecnología que se puedan implementar.

Propuesta de Estructura Organizativa para Departamento de Tecnología y Seguridad Informática en la Cooperativa SIHUACOOP DE R.L.

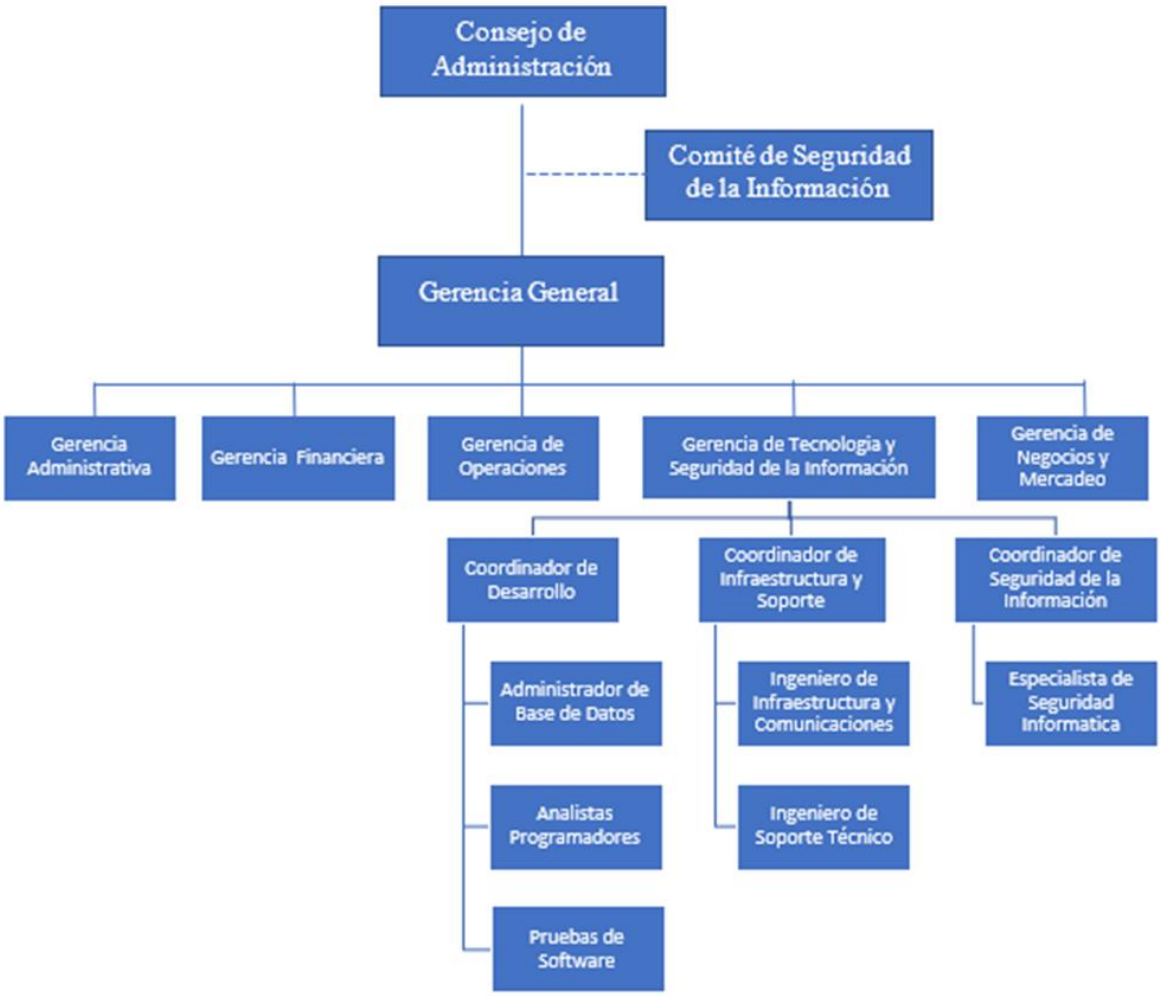


Ilustración 6. Propuesta Estructura organizativa incluyendo SGSI a Largo Plazo. Elaboración propia.

La estructura organizativa para la cooperativa SIHUACOOP DE R.L. a tiempo completo (full-time) del personal en seguridad depende de un número de factores, entre ellos:

- la sensibilidad de la información a ser protegida.
- las regulaciones de las instituciones gubernamentales del país.
- la rentabilidad general.

Organización para el área de la Seguridad de la Información:

- **Comité de Seguridad de Información**
  - o Gerente General (presidente)
  - o Presidente del Consejo de Administración (Administrador)
  - o Gerente Finanzas (miembro)
  - o Gerente de negocios (miembro)
  - o Gerente de Tecnología y seguridad de la información (miembro)
  - o Coordinador de seguridad de la información (secretario)
- **Coordinador del SGSI**

Roles y Responsabilidades de Seguridad de la Información.

- ✓ **Comité de Seguridad de la Información**
  - Se encuentra representado por todos los representantes de las diversas divisiones de la organización.
  - Efectuar la revisión, aprobación y seguimiento de la Política e incidencias de Seguridad de la Información

- ✓ **Coordinador del SGSI**

Principal responsable de la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información en la cooperativa.

- ✓ **Especialista de Seguridad Informática.**

Principal responsable de realizar pruebas a los sistemas, aplicativos, redes etc.; monitorear los eventos de seguridad, encontrar vulnerabilidades y dar una pronta solución.

PUESTOS DE TRABAJO EN EL DEPARTAMENTO DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION:

Tabla 4. Cargo Gerente de Tecnología y Seguridad de la Información.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Gerente de Tecnología y Seguridad de la Información.
Jefe Inmediato: Gerente General.
Descripción del Cargo: Planificar, dirigir, administrar los recursos de Sistemas, Tecnologías y la seguridad de la Información para garantizar las operaciones y la integración de quienes componen las áreas del departamento.

Tabla 5. Cargo Coordinador de Desarrollo de Sistemas.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Coordinador de Desarrollo de Sistemas.
Jefe Inmediato: Gerente de Tecnología y Seguridad de la Información.
Descripción del Cargo: La función principal es coordinar las actividades del personal a cargo como analista programador, administrador de base de datos y pruebas de software y presentar informes a la gerencia de tecnología.

Tabla 6. Cargo Administrador de Base de Datos.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Administrador de Base de Datos.
Jefe Inmediato: Coordinador de Desarrollo de Sistemas.
Descripción del Cargo: Sera el responsable de gestionar, modelar, diseñar, respaldar, auditar, integrar, documentar las diferentes bases de datos que se utilicen en servidores de producción de la cooperativa.

Tabla 7. Cargo Analista-programador.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Analista-programador.
Jefe Inmediato: Coordinador de Desarrollo de Sistemas.
Descripción del Cargo: La función principal es desarrollar aplicaciones y elaborar sistemas informáticos (paquetes de software), así como de implementarlos y ponerlos en marcha, utilizando uno o varios lenguajes de programación.

Tabla 8. Cargo Pruebas de Software.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Pruebas de Software.
Jefe Inmediato: Coordinador de Desarrollo de Sistemas.
Descripción del Cargo: La función principal es realizar pruebas de software y aplicaciones que son implementadas tanto en el Core financiero como nuevos sistemas, presentar informes solicitados.

Tabla 9. Cargo Coordinador de Infraestructura y Comunicaciones.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Coordinador de Infraestructura y Comunicaciones.
Jefe Inmediato: Gerente de Tecnología y Seguridad de la Información.
Descripción del Cargo: La función principal es coordinar las actividades del personal a cargo como Ingeniero de infraestructura, ingeniero de soporte técnico y presentar informes a la gerencia de tecnología.

Tabla 10. Cargo Ingeniero de Soporte Técnico.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Ingeniero de Soporte Técnico.
Jefe Inmediato: Coordinador de Infraestructura y Soporte.
Descripción del Cargo: La función principal es de velar por el correcto funcionamiento de todos los equipos informáticos de la cooperativa, instalar, probar, mantener y actualizar los equipos de los usuarios.

Tabla 11. Cargo Coordinador de Seguridad de la Información.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Coordinador de Seguridad de la Información.
Jefe Inmediato: Gerente de Tecnología y Seguridad de ja Información.
Descripción del Cargo: La función principal es coordinar las actividades del personal a cargo como administrador de seguridad, analista de vulnerabilidades y amenazas, presentar informes a la gerencia de tecnología.

Tabla 12. Cargo Especialista en Seguridad Informática.

Departamento: Tecnología y Seguridad de la Información.
Nombre del Cargo: Especialista en Seguridad Informática.
Jefe Inmediato: Coordinador de Seguridad de la Información.
Descripción del Cargo: La función principal es administrar los recursos y activos de seguridad de la información, realizar actividades de pruebas de penetración a los sistemas, aplicaciones y servidores, monitoreo de eventos para encontrar riesgos sobre vulnerabilidades y amenazas, presentar informes solicitados.

Alcance del SGSI

La Cooperativa SIHUACOOP DE R.L. tiene como propósito establecer un SGSI basado en la norma ISO 27001:2022, para ello es importante realizar la definición de cuáles serán los límites, esto con el objetivo de decidir cuál será la información que se quiere proteger. Cuando se lleve a cabo la clasificación de los activos, se indicará que esa información deberá ser protegida sin importar si es almacenada, procesada, transmitida o transferida dentro o fuera de las instalaciones de la cooperativa.

La SIHUACOOP DE R.L. proporciona los recursos necesarios para establecer un sistema de Gestión de Seguridad de la información que establece los lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información ubicada en los sistemas de información y software que procesen, almacenen y trasmitan información relacionada al proceso financiero, así como a sistemas de información, redes, sistemas operativos, software, hardware, activos tangibles, no tangibles y servicios en la nube. Los aspectos internos y externos relevantes de la organización que se encuentren alineados con la estrategia de negocio y que cumpla con los requisitos de los clientes o asociados, los requisitos de la norma ISO 27001:2022, los requisitos de leyes o regulaciones aplicables.

La protección de todos los activos de información y datos que permiten el desempeño normal y exitoso de las funciones, servicios y actividades de la Cooperativa SIHUACOOP DE R.L. Los activos protegidos en ubicaciones físicas, información impresa, información electrónica, registros, políticas y procedimientos, software y licencias, hardware físico de TI. Los límites para la establecer el SGSI son las ubicaciones físicas, geográficas, los límites organizaciones y los límites de las Tecnologías de la Información y Comunicaciones. Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo con los siguientes aspectos:

Procesos y servicios

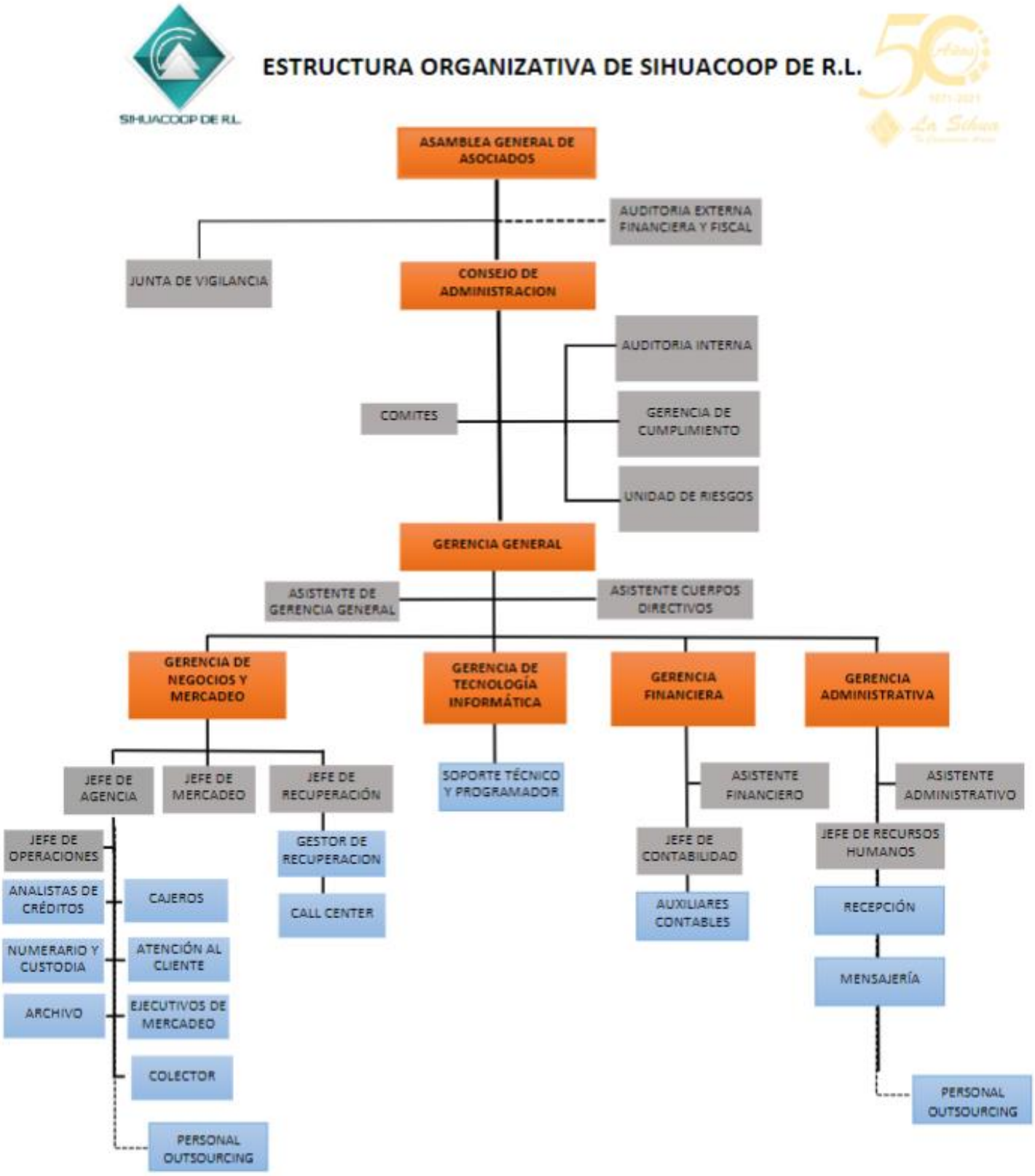
El SGSI aplica a todas las funciones, servicios, actividades y activos de información, que es parte de la cadena de valor definido en el Plan Estratégico Institucional de la SIHUACOOP.

Tabla 13 13.Procesos y servicios

Propietario	Departamento	Activo/Proceso Clave
Programador	Gerencia TI	SIM.NET
Infraestructura	Gerencia TI	Servidor Producción
	Gerencia TI	Servidor Desarrollo
	Gerencia TI	Servidor Mensajería
	Gerencia TI	Servidor de Aplicaciones
	Gerencia TI	Replica Servidor de Aplicaciones
	Gerencia TI	Servidor de Backups
DBA	Gerencia TI	Servidor Base de Datos SQL Server
	Gerencia TI	Replica Servidor Base de Datos SQL Server
Infraestructura	Gerencia TI	Servidor Control de Dominio
	Gerencia TI	Servidor de Correos
	Gerencia TI	Servidor de Telefonía
	Gerencia TI	Servidor Base de Datos Linux
	Gerencia TI	Servidor 1
Soporte	Gerencia TI	Computadora Usuario Final
	Gerencia TI	Router FEDECACES
	Gerencia TI	Router Internet
	Gerencia TI	Enlaces dedicados
	Gerencia TI	Rack de Piso
	Gerencia TI	Switch
	Gerencia TI	UPS Data Center
	Gerencia TI	Planta Eléctrica
	Gerencia TI	NAS
	Gerencia TI	Modem 3G
	Gerencia TI	Gabinete Pared
	Gerencia TI	Sistema de Video Vigilancia
	Gerencia TI	Impresores Multifuncional
	Gerencia TI	Teléfono IP
	Gerencia TI	Firewall
	Gerencia TI	Internet Claro (Turbonett)
Programador	Gerencia TI	WAF
	Gerencia TI	SIHUA-APP
	Gerencia TI	Sihua Online
Soporte	Gerencia TI	Sitio Web lasihua.com
	Gerencia TI	VPN Sucursales
	Gerencia TI	VPN FEDECASES
	Gerencia TI	Respaldo de información
	Gerencia TI	Inventario de Equipos y Licencias
	Gerencia TI	Diagrama de Red
Gerente	Gerencia TI	Políticas de TI y Funciones de Puestos
	Gerencia TI	SIM.NET Manual Técnico
	Gerencia TI	Manuales (Modulo, Seguridad informática, Riesgo de TI)
	Gerencia TI	Plan de Continuidad y Contingencia

Unidades Organizativas

Ilustración 7. Relación Ciclo de Deming con Procesos SGSI



La estructura organizacional de la Seguridad de la Información de SIHUACOOP corresponde al esquema definido y aprobado, en donde se identifican las dependencias funcionales y estratégicas en términos de Seguridad de la Información para la institución. SIHUACCOP en la Gerencia de Tecnología información emplea a una fuerza laboral de 4 para recopilar y procesar información, con el objetivo de permitir la prestación de los servicios.

Ubicaciones

Hay 5 sucursales y un centro financiero en el territorio salvadoreño. Además, algunos funcionarios de SIHUACOOP pueden trabajar desde casa realizando teletrabajo o como trabajadores móviles. La siguiente tabla identifica dónde se pueden ubicar los activos de información:

Tabla 1414. Ubicaciones

SITIO	UBICACION	TIPO DE ACTIVO
Centro financiero	Santa Ana	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.
Sucursal Central Santa Ana	Santa Ana	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.
Sucursal Metapán centro	Metapán	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.
Sucursal Centro comercial El Carmen	Santa Tecla	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.
Sucursal Olímpica	San Salvador	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.
Sucursal Plaza Ferrocarril	Sonsonate	Software, Hardware, Físico, Servicios, Tangible, Intangible, Información.

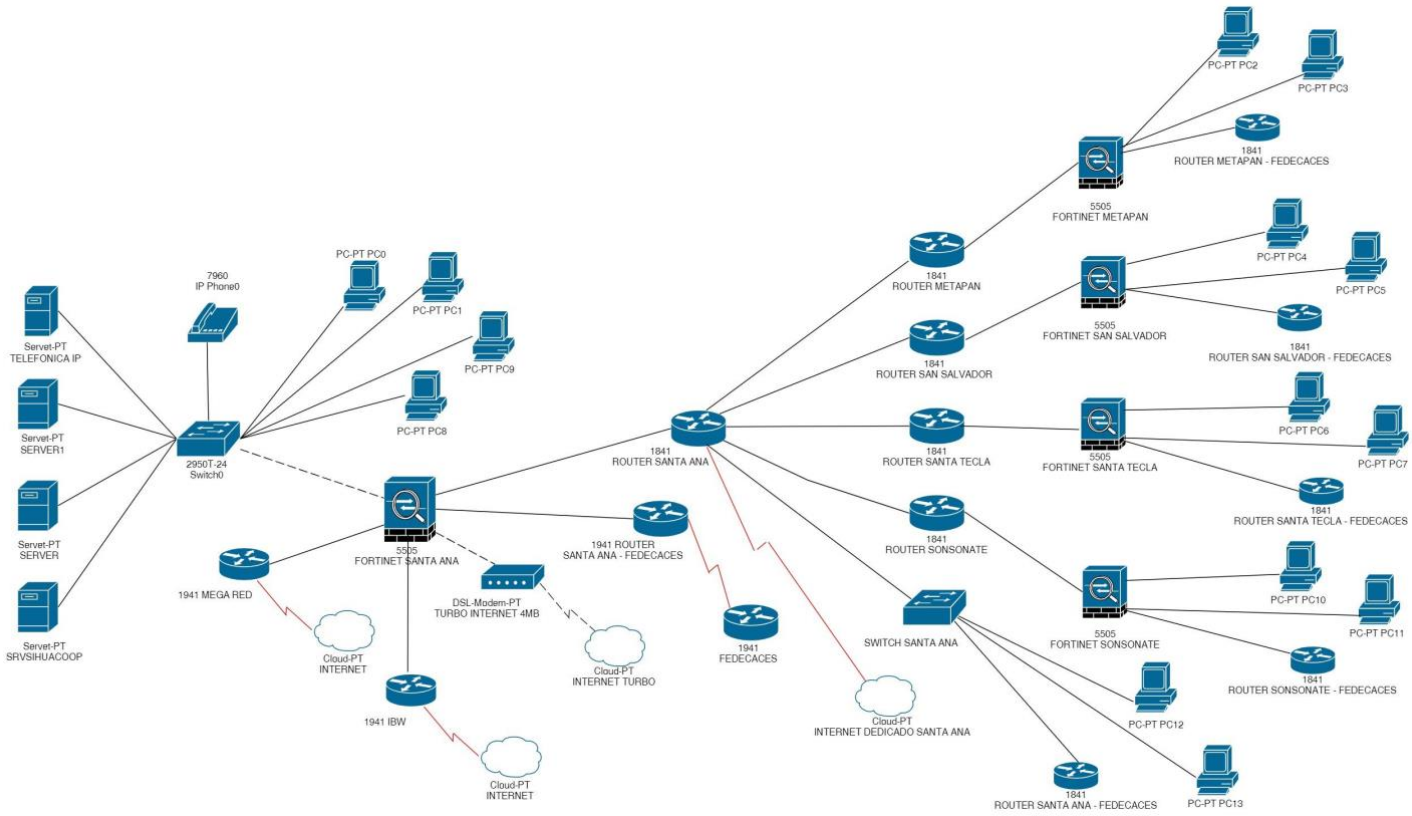
Redes e Infraestructura de TI

Las redes e infraestructuras de TI que están incluidas dentro del alcance se muestran en el siguiente diagrama de Red.

Tabla 1515. Diagrama de Red

Equipo en Diagrama d Red	
Routers	Switches
Servidores	Firewalls
Planta Telefónica	Computadoras de Escritorios
Laptops	Enlaces de Comunicación

Ilustración 8. Diagrama de Red



Exclusiones del Alcance

Los siguientes elementos no están incluidos en el alcance: Activos, Servicios y/o Procesos que no son administrados, gestionados o soportados por la gerencia de TI.

Inventario de activos

Se identifican lista de activos de información a proteger, se brinda una descripción, además se clasifican en Tipo de activo, ubicación, área responsable del mantenimiento y el propietario para cada uno de esos activos. También se valoriza lo crítico o difícil que sería reemplazarlo.

Tabla 1616. Inventarios de Activos

INVENTARIO ACTIVOS SIHUACOOP									**Realizado por:**	**Jaime Avilés, Rodrigo Ayala, Kevin Álvarez**				
									Versión:	**1.0.0**				
		INVENTARIO DE ACTIVOS							**Fecha última actualización:**	**27/08/2023**				
		ASSET INVENTORY							**Revisado por**					
									Aprobado por:					
INVENTARIO										**VALORIZACIÓN**				
Nombre de activo	**Descripción del activo**	**Sistema involucrado**	**Cantidad**	**Tipo de activo**	**Tipo de ubicación**	**Estado del Activo**	**Responsable de Mantenimiento**	**Nivel de confidencialidad**	**Propietario del activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**	**Nivel de tasación**
SIM.NET	Sistema CORE de la organización. SIM.NET (Sistema de Información para Microfinanzas. Network) Sistema desarrollado por FUNDAMICRO (Fundación para Microfinanzas) fundación salvadoreña ubicada en san salvador, proyecto financiado por cooperación española y el BID (Banco Interamericano de Desarrollo) en el año 2011 e implementado en el año 2012; proyecto desarrollado por programadores de FUNDAMICRO y SIHUACOOP hecho en casa y a la medida a las necesidades de la cooperativa. Desarrollado en Visual Studio 2008, con lenguaje de programación Visual Basic.		1	Software	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	5	4	4.33	Muy Alto
Principales Procesos y Cálculos de Formulas del Sistema	Documento que describe las fórmulas de los principales procesos que se llevan a cabo dentro del sistema informático SIM.NET	SIM.NET	1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	3	4	3	3.33	Alto

Descripción de Aspectos Varios	Documento que describe aspectos varios de la infraestructura de TI: - Características de equipo central y periféricos - Características detalladas de la herramienta de desarrollo - Procedimiento autorizado para el manejo de claves de acceso - Normas de higiene para el uso de equipos informáticas y sus periféricos - Licencias de Software a utilizar	SIM.NET	1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	4	3	3	3.33	Alto
Servidor Producción	Hipervisor para virtualización. Windows Server		1	Físico	Física	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	5	5	4	4.67	Muy Alto
Servidor Desarrollo	Servidor Virtual Windows Server	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	3	3	3.33	Alto
Servidor Mensajería	Servidor de Comunicación Interna de la Organización (Chat) Linux Server	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	2	3	3	2.67	Medio
Servidor de Aplicaciones	Servidor Virtualizado Servidor de aplicaciones con servicios IIS y Nginx Microsoft Windows Server 2019 Standard	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
Replica Servidor de Aplicaciones	Replica de aplicaciones para asegurar alta disponibilidad Microsoft Windows Server 2019 Standard	Servidor de Aplicaciones Servidor producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	3	3	3.33	Alto
Servidor de Backups	Microsoft Windows Server 2012 R2 Standard Veeam	Servidor Producción	1	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	5	4	3	4.00	Alto
Servidor Base de Datos SQL Server	Servidor Virtualizado Base de datos donde se almacena la información de los diferentes sistemas que posee la cooperativa Microsoft Windows Server 2019 Standard	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	5	4	4.33	Muy Alto
Replica Servidor Base de Datos SQL Server	Replica de base de datos para asegurar alta disponibilidad Microsoft Windows Server 2019 Standard	Servidor Base de Datos SQL Server Servidor producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	5	3	4.00	Alto
Servidor Control de Dominio	Servidor en la Nube Microsoft Windows Server 2019 Standard		1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto

Servidor de Correos	Servidor Virtualizado Servidor Zimbra Servidor Linux	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	2	3	3	2.67	Medio
Servidor de Telefonía	Servidor Virtualizado Utilizado para call center. Servidor Linux	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
Servidor Base de Datos	Servidor Linux Ubuntu Server	Servidor Producción	1	Intangibles	Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
Servidor 1	Microsoft® Windows Server® 2008 Enterprise		1	Físico	Lógica	Fuera de Servicio	Departamento TI	Confidencial de la compañía	Departamento TI	4	2	2	2.67	Medio
Computadora Usuario Final	Microsoft Windows 10 Pro		112	Físico	Física	En Uso	Departamento TI	Confidencial de los empleados	Organización	2	3	3	2.67	Medio
Computadora Usuario Final	Microsoft Windows 7 Professional		2	Físico	Física	En Uso	Departamento TI	Confidencial de los empleados	Organización	2	3	3	2.67	Medio
Router FEDECACES	Router encargado de establecer red privada de datos con FEDECACES, Ancho de banda 3MiB Administrado por el proveedor		6	Físico	Física	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	3	3.67	Alto
Router Internet	Router encargado de proporcionar Internet dedicado y conexión con otras agencias		5	Físico	Física	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
Enlaces dedicados	Enlaces de contingencia IBW MEGARED		2	Físico	Física	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	3	3.67	Alto
Rack de Piso	Soporta 4 patch panels de 24 puertos c/u, cuatro switches de 24 puertos c/u, dos routers y un firewall		1	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	3	4	3.33	Alto
Switch	Dispositivo de acceso a red para los equipos institucionales tanto en central como en sucursales. Conexión de Telefonía IP.		6	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	4	3	3.33	Alto
UPS Data Center			2	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	4	4	3.67	Alto
Planta Eléctrica	Utilizada como soporte en caso de falta de suministro eléctrico.		1	Físico	Físico	En Uso	Administración	Confidencial de la compañía	Organización	2	4	4	3.33	Alto
NAS	Almacenamiento en red		2	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Organización	4	4	4	4.00	Alto
Modem 3G	Contingencia en caso de perder conectividad en enlaces principales		5	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Organización	3	3	2	2.67	Medio
Gabinete Pared	Para almacenamiento de los dispositivos de red de cada agencia.		5	Físico	Físico	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	3	3	3.00	Medio

Sistema de Video Vigilancia	Sistema utilizado para monitoreo físico de las instalaciones de la central y sucursales.		5	Físico	Físico	En Uso	Proveedor	Confidencial de la compañía	Organización	4	2	3	3.00	Medio
Impresores Multifuncional	Impresores utilizados para impresión de contratos, facturas y documentación para procesos operacionales de la organización.		6	Físico	Físico	En Uso	Proveedor	Confidencial de la compañía	Organización	2	3	4	3.00	Medio
Teléfono IP	Dispositivos para audio comunicación interna.			Físico	Físico	En Uso	Departamento TI	Confidencial de los empleados	Organización	2	3	3	2.67	Medio
Firewall	Dispositivo Fortinet que funciona como Firewall, Anti-Spam y Antivirus. Permite establecer reglas de navegación para Internet, es utilizado además para establecer una VPN con las demás agencias.		5	Físico	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
Internet Claro (Turbonett)	Servicio de Internet para brindar acceso a personal e invitados. Esta red es adicional al internet dedicado para evitar la degradación del mismo.		1	Servicios	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	2	3	3	2.67	Medio
WAF	Web Application Firewall o en español: Firewall de Aplicaciones Web	SIM.NET Sihua Online Sitio Web lasihua.com	1	Software	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
SIHUA-APP	Aplicación móvil disponible para asociados de la cooperativa y donde pueden realizar solicitudes y transacciones de los productos ofrecidos por la cooperativa. Disponible para Android y Apple	Servidor Producción	1	Software	Lógica	En Uso	Departamento TI	Confidencial del cliente	Departamento TI	3	4	4	3.67	Alto
Sihua Online	Plataforma web que permite a asociados consultar sus servicios (cuenta de ahorro, transferencias, pago de créditos, depósitos a plazo)	Servidor de Aplicaciones IIS	1	Software	Lógica	En Uso	Departamento TI	Confidencial del cliente	Departamento TI	3	4	4	3.67	Alto
Sitio Web lasihua.com	Sitio Web disponible al todo público para mostrar información de la cooperativa, servicios que ofrece e información relevante para futuros asociados y asociados vigentes.	Servidor de Aplicaciones Nginx	1	Software	Lógica	En Uso	Departamento TI	No clasificado	Departamento TI	1	4	3	2.67	Medio
VPN Sucursales	Conexiones VPN desde la central con las diferentes sucursales a nivel nacional.		5	Servicios	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	4	4	4	4.00	Alto
VPN FEDECASES	Conexión VPN para comunicación con red de Cooperativas FEDECACES		5	Servicios	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	3	3	3.00	Medio
Copias de Respaldo	Copias de la base de datos almacenadas en físico y en la nube para realizar restauraciones a puntos anteriores en el tiempo en caso de ser necesario		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	5	5	5	5.00	Muy Alto
Inventario de Equipos y Licencias	Inventario de licencias de equipos, Microsoft office, antivirus entre otros.		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	5	3	3.67	Alto
Diagrama de Red	Diagrama Topológico de Red entre las oficinas centrales y las 4 sucursales de la cooperativa		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de la compañía	Departamento TI	3	3	3	3.00	Medio

Funciones de Puestos TI	Descripción de los puestos actuales en el departamento, funciones específicas y conocimientos requeridos.		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	2	3	2	2.33	Medio
SIM.NET Manual Técnico	Descripción técnica de las funciones, controles y pantallas del sistema.	SIM.NET	1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	2	4	2	2.67	Medio
Manuales por Modulo	Descripción de cada módulo del sistema y su funcionalidad básica.	SIM.NET	1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	2	4	2	2.67	Medio
Plan de Continuidad y Contingencia	Documento que contiene estrategia de recuperación en caso de materializarse un desastre evaluado previamente.	SIM.NET	1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	4	4	3	3.67	Alto
Política de Tecnología de Información	política interna de las normas a seguir en materia de Tecnología.		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	2	4	3	3.00	Medio
Manual de Administración de Seguridad Informática, Calves, Permisos y Accesos	Manual que expone procedimientos aprobados para el correcto tratamiento de credenciales, permisos y gestión de seguridad.		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	2	4	3	3.00	Medio
Manual de Gestión de Riesgo Tecnológico	Manual que contiene detalles sobre cómo gestionar los riesgos que se relacionan a los servicios de TI.		1	Información	Física-Lógica	En Uso	Departamento TI	Confidencial de los empleados	Departamento TI	4	4	3	3.67	Alto

Valoración e identificación de activos de acuerdo con el impacto

Para cada activo definido identificaremos los riesgos y los clasificaremos en función de su gravedad y vulnerabilidad. Además, identificaremos el impacto que la pérdida de confidencialidad, integridad y disponibilidad que puede tener en los activos.

Veamos de forma inicial el sistema de valorización y clasificación que tomaremos en cuenta para el desarrollo de la valoración, el cual se enfoca en los tres pilares de Seguridad:

Tabla 1717. Clasificación Tipo de Activo

Activos		Descripción
Tipo de activos	Información	Bases de datos, archivos, documentación del sistema, manuales, material de capacitación, procedimientos de contingencia, etc.
	Software	Aplicaciones, desarrollos, utilitarios, herramientas de desarrollo, etc.
	Físico	Equipos de comunicaciones, equipo de cómputo, gabinetes, ups, dispositivos, etc.
	Intangibles	Reputación, imagen.
	Personas	Capital humano, habilidades, experiencia.
	Servicios	servicios de comunicaciones, servicios necesarios para la ejecución del negocio.

Tabla 1818. Referencia para Valorización de Confidencialidad.

	Valor de Activo	Descripción
Confidencialidad	5 (Muy Alto)	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.
	4 (Alto)	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la organización.
	3 (Medio)	La información asociada al activo es confidencial y solo personal de algunas áreas internas pueden acceder a ella, pues su divulgación afectaría considerablemente a la organización.
	2 (Bajo)	La información asociada al activo es de uso interno y solo personal de ABC puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.
	1 (Muy Bajo)	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización.

Tabla 1919. Referencia para Valorización de Integridad.

	Valor de Activo	Descripción
Integridad	5 (Muy Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría irreversiblemente a la organización.
	4 (Alto)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15%, pues la vulneración de su integridad afectaría gravemente a la organización.
	3 (Medio)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la organización.
	2 (Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la organización.
	1 (Muy Bajo)	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la organización.

Tabla 2020. Referencia para Valorización de Disponibilidad.

	Valor de Activo	Descripción
Disponibilidad	5 (Muy Alto)	Se requiere que el activo nunca se encuentre indisponible, pues su carencia afectaría irreversiblemente a la organización.
	4 (Alto)	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la organización.
	3 (Medio)	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.
	2 (Bajo)	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la organización.
	1 (Muy Bajo)	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.

Para la estimación del Valor del activo, se tomará el promedio de los valores de nivel de importancia de la Confidencialidad, Integridad y Disponibilidad.

Una vez teniendo ese promedio, el nivel del impacto se estimará en base al valor promedio obtenido.

Tabla 2121. Nivel de Impacto en base a valoración promedio del activo.

Valor promedio del Activo	Nivel de Impacto

4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
1.000 – 1.000	Muy Bajo

Realicemos una valoración para comprender mejor este sistema; tomemos como ejemplo el activo: **SIM.NET.** Para el cual estableceremos la importancia de la confidencialidad como Alto (4), Integridad se considera Muy Alto (5) dado que es el sistema CORE y finalmente Disponibilidad como Alto (4) ya que las operaciones no pueden continuar si dicho activo.

El Valor se determinará entonces:

$$Valor = \frac{Confidencialidad + Integridad + Disponibilidad}{3} = \frac{4 + 5 + 4}{3} = \frac{13}{3} \approx 4.33$$

Dado que el valor aproximado es **4.33**, se estima el Nivel de Impacto como **Muy Alto**. Este proceso se repite de igual forma para todos los activos, tomando en cuenta las características de estos para establecer valores de Confidencialidad, Integridad y Disponibilidad acordes a la naturaleza e importancia dentro de la Cooperativa.

Tabla 2222. Activos x impacto

No	Activo	Tipo Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Nivel de Impacto
1	SIM.NET	Software	4	5	4	4.33	Muy Alto
2	Principales Procesos y Cálculos de Formulas del Sistema	Información	3	4	3	3.33	Alto
3	Descripción de Aspectos Varios	Información	4	3	3	3.33	Alto
4	Servidor Producción	Físico	5	5	4	4.67	Muy Alto
5	Servidor Desarrollo	Intangibles	4	3	3	3.33	Alto
6	Servidor Mensajería	Intangibles	2	3	3	2.67	Medio
7	Servidor de Aplicaciones	Intangibles	4	4	4	4.00	Alto
8	Replica Servidor de Aplicaciones	Intangibles	4	3	3	3.33	Alto
9	Servidor de Backups	Físico	5	4	3	4.00	Alto
10	Servidor Base de Datos SQL Server	Intangibles	4	5	4	4.33	Muy Alto
11	Replica Servidor Base de Datos SQL Server	Intangibles	4	5	3	4.00	Alto
12	Servidor Control de Dominio	Intangibles	4	4	4	4.00	Alto
13	Servidor de Correos	Intangibles	2	3	3	2.67	Medio
14	Servidor de Telefonía	Intangibles	4	4	4	4.00	Alto
15	Servidor Base de Datos Linux	Intangibles	4	4	4	4.00	Alto
16	Servidor 1	Físico	4	2	2	2.67	Medio
17	Computadora Usuario Final	Físico	2	3	3	2.67	Medio
18	Router FEDECACES	Físico	4	4	3	3.67	Alto
19	Router Internet	Físico	4	4	4	4.00	Alto
20	Enlaces dedicados	Físico	4	4	3	3.67	Alto
21	Rack de Piso	Físico	3	3	4	3.33	Alto

22	Switch	Físico	3	4	3	3.33	Alto
23	UPS Data Center	Físico	3	4	4	3.67	Alto
24	Planta Eléctrica	Físico	2	4	4	3.33	Alto
25	NAS	Físico	4	4	4	4.00	Alto
26	Modem 3G	Físico	3	3	2	2.67	Medio
27	Gabinete Pared	Físico	3	3	3	3.00	Medio
28	Sistema de Video Vigilancia	Físico	4	2	3	3.00	Medio
29	Impresores Multifuncional	Físico	2	3	4	3.00	Medio
30	Teléfono IP	Físico	2	3	3	2.67	Medio
31	Firewall	Físico	4	4	4	4.00	Alto
32	Internet Claro (Turbonett)	Servicios	2	3	3	2.67	Medio
33	WAF	Software	4	4	4	4.00	Alto
34	SIHUA-APP	Software	3	4	4	3.67	Alto
35	Sihua Online	Software	3	4	4	3.67	Alto
36	Sitio Web lasihua.com	Software	1	4	3	2.67	Medio
37	VPN Sucursales	Servicios	4	4	4	4.00	Alto
38	VPN FEDECASES	Servicios	3	3	3	3.00	Medio
39	Respaldo de información	Información	5	5	5	5.00	Muy Alto
40	Inventario de Equipos y Licencias	Información	3	5	3	3.67	Alto
41	Diagrama de Red	Información	3	3	3	3.00	Medio
42	Funciones de Puestos TI	Información	2	3	2	2.33	Medio
43	SIM.NET Manual Técnico	Información	2	4	2	2.67	Medio
44	Manuales por Modulo	Información	2	4	2	2.67	Medio
45	Plan de Continuidad y Contingencia	Información	4	4	3	3.67	Alto
46	Política de Tecnología de Información	Información	2	4	3	3.00	Medio
47	Manual de Administración de Seguridad Informática, Calves, Permisos y Accesos	Información	2	4	3	3.00	Medio
48	Manual de Gestión de Riesgo Tecnológico	Información	4	4	3	3.67	Alto

Identificación de los requisitos de cumplimientos

El **Cumplimiento** implica satisfacer los requisitos para cumplir las obligaciones normativas, legales o con los clientes de la cooperativa. La identificación de los controles en los riesgos que se evalúen en los activos y que se utilicen en el análisis dependerá de la naturaleza de las actividades de negocios de cada organización.

La fase de identificación de los requisitos de cumplimiento es aquella donde todas las políticas escritas o que se estipulan en el diseño del SGSI basado en la norma ISO 27001:2022, deben

ser implementados y estar relacionados con los controles de seguridad de la información, ya que esto permitirá que exista una base sólida entre los que se diseña versus los controles de seguridad ya implementados y posteriormente documentados.

El incumplimiento de las leyes, regulaciones o políticas internas relacionadas con la seguridad de la información puede generar sanciones legales o dañar la reputación de la organización.

Ejemplo: Identificando las secciones de los controles como: organizacionales, físicos y de personas, los cuales fueron seleccionados según la evaluación de riesgos que se realizó a cada activo que contiene la cooperativa, basándonos según la documentación que tiene en seguridad de la información, políticas, procesos, procedimientos, auditorias, etc. Para el caso del control A5.2 Funciones y responsabilidades de seguridad de la información, es porque la organización tiene debilidades en las funciones asignadas a cada puesto de trabajo, porque todos realizan actividades de los puestos que están vacantes o que no están definidos en la cooperativa, por lo tanto, ha salido como un control que se debe mejorar por mostrarse deficiente.

Detalle de controles donde salieron deficientes en la evaluación para el Nivel MMC 0, 1, 2 y que podrían ser mejorados los controles en la Cooperativa.

Tabla 2323. Requisitos de cumplimiento

Estándar	Sección	
A.5 Controles Organizacionales		
A5.2	Funciones y responsabilidades de seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
A5.4	Responsabilidades de gestión	**Control** La gerencia requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos del tema de la organización.
A5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
A5.7	Inteligencia de amenazas	**Control** La información relativa a las amenazas a la seguridad de la información se recopilará y analizará para producir información sobre amenazas.
A5.8	Seguridad de la información en la gestión de proyectos	**Control** La seguridad de la información se integrará en la gestión del proyecto.
A5.11	Devolución de activos	**Control** El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su poder al cambiar o terminar su empleo, contrato o acuerdo.
A5.13	Etiquetado de la información	**Control** Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.
A5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	**Control** Los requisitos pertinentes de seguridad de la información se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.
A5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la	**Control** Deben definirse y aplicarse procesos y procedimientos implantados para gestionar los riesgos de seguridad de la

	información y la comunicación (TIC)	información asociados a la cadena de suministro de productos y servicios de TIC.
A5.22	Monitoreo, revisión y gestión del cambio de los servicios de los proveedores	**Control** La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
A5.23	Seguridad de la información para el uso de servicios en la nube	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización.
A5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	**Control** La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.
A5.25	Evaluación y decisión sobre eventos de seguridad en la información	**Control** La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.
A5.26	Respuesta a incidentes de seguridad de la información	**Control** Los incidentes de seguridad de la información se responderán de acuerdo con los procedimientos documentados.
A5.27	Aprender de los incidentes de seguridad de la información	**Control** Los conocimientos adquiridos en los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.
A5.28	Obtención de pruebas	**Control** La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
A5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	**Control** Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.

A5.34	Privacidad y protección de la información de identificación personal (PII)	**Control** La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de Pll de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
A5.35	Examen independiente de la seguridad de la información	**Control** El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
A5.36	Cumplimiento de políticas, reglas y estándares para la seguridad de la información	**Control** El cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos del tema se revisarán regularmente.
A.6 Controles de personas		
A6.8	Informes de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados de manera oportuna.
A.7 Controles Físicos		
A7.7	Escritorio claro y pantalla clara	**Control** Se definirán y aplicarán adecuadamente normas de escritorio claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas para las instalaciones de tratamiento de la información.

Identificación de amenazas y vulnerabilidades

Empezaremos por identificar las amenazas y vulnerabilidades reales o potenciales de cada activo detallados en la identificación y valoración de activos.

Antes vamos a definir conceptos claves para poder comprender más fácil esta parte.

Vulnerabilidad: Es una debilidad o falla en el sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Amenaza: Es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Las **vulnerabilidades** están en directa interrelación con las **amenazas** porque si no existe una **amenaza**, tampoco existe la **vulnerabilidad**, o bien, pierde importancia, porque no se puede ocasionar un daño.

La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

Ejemplo:

Imaginemos un dispositivo obsoleto de comunicaciones en una red corporativa, podríamos decir que supone una amenaza para la cooperativa, pero supone también una vulnerabilidad. Si consideramos que el dispositivo puede provocar daños a la cooperativa (perdida de información, bajo rendimiento, etc.). Si por el contrario consideramos que puede suponer un riesgo por favorecer los ataques, entonces, sería más bien una vulnerabilidad. En ambos casos, el denominador común es un riesgo o daño para la cooperativa, uno de forma directa y otro de forma indirecta.

En la siguiente tabla mostraremos las amenazas y vulnerabilidades potenciales según nuestro análisis.

Tabla 2424. Amenaza y vulnerabilidad

Amenazas	Vulnerabilidad
[E.1] Errores de los usuarios	Error en el uso de servicios o datos.
[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.
[E.8] Difusión de software dañino	Propagación inocente de virus.
[E.15] Alteración accidental de la información	Alteración accidental de la información.
[E.18] Destrucción de información	Eliminación intencional de información.
[E.19] Fugas de información	revelación de la información por indiscreción.

[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario.
[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software.
[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios.
[A.6] Abuso de privilegios de acceso	Abuso de derechos.
[A.8] Difusión de software dañino	Propagación intencionada de virus.
[A.11] Acceso no autorizado	Uso ilícito del hardware.
[A.15] Modificación deliberada de la información	Alteración intencional de la información.
[A.18] Destrucción de información	Pérdida accidental de información.
[A.19] Divulgación de información	Copia ilegal de software.
[A.22] Manipulación de programas	alteración intencionada de los datos.
[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema.
[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema.
[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electromagnéticos.
[I.5] Avería de origen físico o lógico	avería o falla en el funcionamiento del hardware.
[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.
[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.
[E.4] Errores de configuración	introducción de datos errores
[E.24] Caída del sistema por agotamiento de recursos	saturación del sistema informático
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas.
[A.23] Manipulación de los equipos	Sabotaje del hardware
[A.24] Denegación de servicio	saturación del sistema informático.
[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios.
[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware.
[E.25] Pérdida de equipos	Recuperación de soportes reciclados.
[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de telecomunicación.
[A.3] Manipulación de los registros de actividad (log)	alteración o eliminación de registros.
[A.9] [Re-]encaminamiento de mensajes	desviación de mensajes que llegue a un destino fraudulento.
[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje.
[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde.
[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar para extraer información y hacer conclusiones.
[I.6] Corte del suministro eléctrico	Perdida del suministro de energía.

Evaluación de riesgos y tratamiento

La identificación de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Una vez que tenemos clara la diferencia entre amenaza y vulnerabilidad, es interesante introducir el concepto de riesgo.

Riesgo: Es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños.

Código: Es el identificador o correlativo que con el cual hemos identificado los riesgos.

Evaluación de riesgos

Una vez identificados los riesgos y los niveles de confidencialidad, integridad y disponibilidad, tendrá que asignar valores a los riesgos. Los valores le ayudarán a determinar si el riesgo es tolerable o no y si necesita implantar un control para eliminarlo o reducirlo. Para asignar valores a los riesgos, hay que tener en cuenta:

- El valor del activo protegido
- La frecuencia con la que puede producirse la amenaza o vulnerabilidad.
- El daño que el riesgo podría infringir a la empresa o a sus socios.

Definimos los criterios de riesgo de seguridad de la información, incluyendo los criterios de aceptación del riesgo y los criterios para realizar evaluaciones de riesgos de seguridad de la información. Aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información. Además, se incluye la identificación de los propietarios del riesgo.

Ejemplo: Imaginémonos la Sihua Online gestiona información confidencial (nombres, contraseñas, cuentas bancarias, etc.). Si los sistemas de dichos sitios no se encuentran actualizados y no implementan medidas de protección adecuadas, podríamos decir que esos sitios son vulnerables a determinadas amenazas, y, por tanto, un alto riesgo de ser susceptibles de recibir ataques.

En cambio, si los sitios web implementan las medidas oportunas y se encuentran actualizados, podrían no ser vulnerables a esas amenazas, pero no estarían exentos del riesgo de sufrir un ataque, causado, por ejemplo, por un ciber atacante que utilice la ingeniera social contra un usuario de la cooperativa para conseguir información privilegiada.

En la siguiente tabla se muestra el valor que se asigna segun clasificación con el criterio que definimos de probabilidad de ocurrencia.

Tabla 2525. Criterio de Probabilidad de Riesgo

Valor	Clasificación	Criterio
5	Probable	Alta probabilidad de ocurrencia, podría ocurrir en semanas a meses.
4	Posible	Significativa probabilidad de ocurrencia, podría ocurrir en semanas a meses.
3	Improbable	Puede ocurrir, pero no a menudo, podría no ocurrir en semanas a meses.
2	Raro	Limitada probabilidad de ocurrencia, podría ocurrir en pocas circunstancias.
1	Remoto	Baja probabilidad de que ocurra, puede ocurrir en ocasiones excepcionales.

Se analizan los riesgos de seguridad de la información para evaluar las consecuencias potenciales que resultarían si los riesgos identificados se materializaran; para evaluar la probabilidad de ocurrencia de los riesgos; y la determinación del nivel de riesgo.

Para ello hemos definido la siguiente tabla donde entenderemos mejor el criterio que utilizaremos para la consecuencia:

Tabla 2626. Criterio de Consecuencia

Valor	Criterio
MA (Muy Alto)	Los riesgos muy altos o extremos deben ponerse en conocimiento de los directores y ser objeto de seguimiento permanente.
A(Alto)	Los riesgos altos requieren la atención de presidente /director general /director ejecutivo.
M(Medio)	Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.
B(Bajo)	Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.
MB (Muy Bajo)	Estos riesgos muy bajos, no necesariamente se deben monitorear de forma continua, pero siempre se debe estar pendiente.

Se identifican la probabilidad de que un riesgo ocurra al realizar el cruce de la consecuencia con la probabilidad como se muestra en la siguiente tabla.

Tabla 2727 Probabilidad y Consecuencia

Código de Riesgo	Categoría de Amenazas	Amenazas	Consecuencia	Probabilidad
R1	[N] Desastres naturales	[N.1] Fuego	6	1
R2		[N.2] Daños por agua	6	2
R3		[N.*] Desastres naturales	3	3
R4	[I] De origen industrial	[I.1] Fuego	6	2
R5		[I.2] Daños por agua	5	3
R6		[I.*] Desastres industriales	3	3
R7		[I.3] Contaminación mecánica	1	3
R8		[I.4] Contaminación electromagnética	2	2
R9		[I.5] Avería de origen físico o lógico	4	2
R10		[I.6] Corte del suministro eléctrico	3	4
R11		[I.7] Condiciones inadecuadas de temperatura o humedad	4	4
R12		[I.8] Fallo de servicios de comunicaciones	4	4
R13		[I.9] Interrupción de otros servicios y suministros esenciales	1	2
R14		[I.10] Degradación de los soportes de almacenamiento de la información	3	3
R15		[I.11] Emanaciones electromagnéticas	2	1
R16	[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios	3	4
R17		[E.2] Errores del administrador	4	3
R18		[E.3] Errores de monitorización (log)	2	3
R19		[E.4] Errores de configuración	3	3
R20		[E.7] Deficiencias en la organización	3	4
R21		[E.8] Difusión de software dañino	5	5
R22		[E.9] Errores de [re-]encaminamiento	3	2
R23		[E.10] Errores de secuencia	2	2
R24		[E.15] Alteración accidental de la información	4	2
R25		[E.18] Destrucción de información	4	1
R26		[E.19] Fugas de información	5	4

R27		[E.20] Vulnerabilidades de los programas (software)	5	4
R28		[E.21] Errores de mantenimiento / actualización de programas (software)	3	4
R29		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	2
R30		[E.24] Caída del sistema por agotamiento de recursos	5	3
R31		[E.25] Pérdida de equipos	3	3
R32		[E.28] Indisponibilidad del personal	2	4
R33	[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	2	1
R34		[A.4] Manipulación de la configuración	3	2
R35		[A.5] Suplantación de la identidad del usuario	4	4
R36		[A.6] Abuso de privilegios de acceso	3	4
R37		[A.7] Uso no previsto	2	5
R38		[A.8] Difusión de software dañino	3	4
R39		[A.9] [Re-]encaminamiento de mensajes	3	4
R40		[A.10] Alteración de secuencia	3	4
R41		[A.11] Acceso no autorizado	3	4
R42		[A.12] Análisis de tráfico	2	4
R43		[A.13] Repudio	2	3
R44		[A.14] Interceptación de información (escucha)	3	4
R45		[A.15] Modificación deliberada de la información	4	3
R46		[A.18] Destrucción de información	5	4
R47		[A.19] Divulgación de información	5	4
R48		[A.22] Manipulación de programas	5	3
R49		[A.23] Manipulación de los equipos	2	3
R50		[A.24] Denegación de servicio	5	4
R51		[A.25] Robo	4	4
R52		[A.26] Ataque destructivo	4	4
R53		[A.27] Ocupación enemiga	3	2
R54		[A.28] Indisponibilidad del personal	3	3
R55		[A.29] Extorsión	4	4
R56		[A.30] Ingeniería social (picaresca)	4	5

Tabla28 28. Matriz de Consecuencia y Probabilidad

Clasificación de Probabilidad							
	5		R37		R56	R21	
	4		R32, R42	R10, R16, R20, R28, R36, R38, R39, R40, R41, R44	R11, R12, R35, R51, R52, R55	R26, R27, R46, R47, R50	
	3	R7	R18, R43, R49	R3, R6, R14, R19, R31, R54	R17, R45	R5, R30, R48	
	2	R13	R8, R23	R22, R29, R34, R53	R9, R24		R2, R4
	1		R15, R33		R25		R1
		1	2	3	4	5	6
		Clasificación de Consecuencia					

Ejemplo:

En el caso de **R21** es el identificador del riesgo asociado al activo que definimos anteriormente, la probabilidad de que este ocurra, la **difusión de software dañino** que es una amenaza que está clasificada como Errores o fallos no intencionados, la vulnerabilidad que no es más que un agujero o falla en este caso es la **propagación inocente de virus** una debilidad que se debe mitigar estableciendo un control.

Tabla 2929 Aplicación de controles a vulnerabilidades y amenazas

Activo	Código Riesgo	Amenazas	Vulnerabilidad	Controles aplicar	Riesgo
SIM.NET	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M

	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
Servidor Producción	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B

	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A

	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA

	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M

	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A

	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor Mensajería	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de	Falla en el funcionamiento del hardware por	A7.10 Medios de almacenamiento	M

		almacenamiento de la información	consecuencia del paso del tiempo.		
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M

	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A

	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M

	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A

	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Replica Servidor de Aplicaciones	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con	A8.15 Registro.	A

			responsabilidades de instalación y operación		
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas,	A

				salas e instalaciones. A8.24 Uso de criptografía.	
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor de Backups	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los	A7.5 Protección contra amenazas físicas y ambientales.	A

			equipos a excesivo calor, frio o humedad.		
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M

	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor Base de Datos SQL Server	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA

	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario.	M

				A5.10 Uso aceptable de la información y otros activos asociados.	
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A

	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Replica Servidor Base de Datos SQL Server	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados	M

				A6.4 Proceso disciplinario	
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B

	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor Control de Dominio	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B

	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A

	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA

Servidor de Correos	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M

	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A

	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor de Telefonía	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de	Falla en el funcionamiento del hardware por	A7.10 Medios de almacenamiento	M

		almacenamiento de la información	consecuencia del paso del tiempo.		
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M

	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Servidor Base de Datos Linux	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A

	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M

	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A

	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Computadora Usuario Final	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con	A8.15 Registro.	A

			responsabilidades de instalación y operación		
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R31	[E.25] Pérdida de equipos	Recuperación de soportes reciclados	A8.5 Autenticación segura.	M
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA

	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Router FEDECACES	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M

	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA

	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llegue a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R44	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde	A8.21 Seguridad en los servicios de red	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A

	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Router Internet	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo	A

				A7.12 Seguridad del cableado	
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento /	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de	M

		actualización de equipos (hardware)		software en sistemas operativos	
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R44	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde	A8.21 Seguridad en los servicios de red	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A

	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Enlaces dedicados	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados	M

				A6.4 Proceso disciplinario	
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M

	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R42	[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar para extraer información y hacer conclusiones	A8.16 Actividades de supervisión	M
	R44	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde	A8.21 Seguridad en los servicios de red	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación	MA

				sobre seguridad de la información.	
Switch	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con	A8.15 Registro.	A

			responsabilidades de instalación y operación		
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R44	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde	A8.21 Seguridad en los servicios de red	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B

	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
UPS Data Center	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B

	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R10	[I.6] Corte del suministro eléctrico	Perdida del suministro de enenergía7.11 Utilidades de apoyo	M	
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de	A

				registros A5.15 Control de acceso	
Planta Eléctrica	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R10	[I.6] Corte del suministro eléctrico	Perdida del suministro de energía	A7.11 Utilidades de apoyo	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B

	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
NAS	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A

	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M

	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Sistema de Video Vigilancia	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA

	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M

	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.	A

				A8.24 Uso de criptografía.	
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
Firewall	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A

	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB

	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R42	[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar extraer hacerse conclusiones	A8.16 Actividades de supervisión	M
	R44	[A.14] Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde	A8.21 Seguridad en los servicios de red	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R49	[A.23] Manipulación de los equipos	Sabotaje del hardware	A7.2 Entrada física	B
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las	A8.21 Seguridad en los servicios de red A7.2 Entrada física	A

			personas, destrucción de Hardware	A5.33 Protección de registros A5.15 Control de acceso	
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
WAF	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
	R8	[I.4] Contaminación electromagnética	Daño en equipo por exposición a emisiones electromagnéticas y radiaciones térmicas e impulsos electro	A7.5 Protección contra amenazas físicas y ambientales.	B
	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A

	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA
	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M

	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R42	[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar para extraer información y hacer conclusiones	A8.16 Actividades de supervisión	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
SIHUA-APP	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA

	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación	MA

				sobre seguridad de la información.	
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
Sihua Online	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA

	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
Sitio Web lasihua.com	R16	[E.1] Errores de los usuarios	Error en el uso de servicios o datos	A5.10 Uso aceptable de la información y otros activos asociados A6.4 Proceso disciplinario	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con	A8.15 Registro.	A

			responsabilidades de instalación y operación		
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A

	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
VPN Sucursales	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA

	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R42	[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar para extraer información y hacer conclusiones	A8.16 Actividades de supervisión	M

	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
VPN FEDECASES	R9	[I.5] Avería de origen físico o lógico	Avería o falla en el funcionamiento del hardware	A7.5 Protección contra amenazas físicas y ambientales.	M
	R11	[I.7] Condiciones inadecuadas de temperatura o humedad	Fallas en la climatización que puede exponer a los equipos a excesivo calor, frio o humedad.	A7.5 Protección contra amenazas físicas y ambientales.	A
	R12	[I.8] Fallo de servicios de comunicaciones	Perdida de los medios de Telecomunicación	A7.11 Utilidades de apoyo A7.12 Seguridad del cableado	A
	R14	[I.10] Degradación de los soportes de almacenamiento de la información	Falla en el funcionamiento del hardware por consecuencia del paso del tiempo.	A7.10 Medios de almacenamiento	M
	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R19	[E.4] Errores de configuración	introducción de datos erróneos	A8.9 Gestión de la configuración.	M
	R21	[E.8] Difusión de software dañino	Propagación inocente de virus	A8.7 Protección contra malware.	MA

	R27	[E.20] Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario	A8.25 Ciclo de vida de desarrollo seguro. A8.29 Pruebas de seguridad en desarrollo y aceptación.	MA
	R28	[E.21] Errores de mantenimiento / actualización de programas (software)	Falle en el funcionamiento del software	A8.19 Instalación de software en sistemas operativos.	M
	R29	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Perjuicio a dar mantenimiento a los sistemas	A7.13 Mantenimiento de equipos A8.19 Instalación de software en sistemas operativos	M
	R30	[E.24] Caída del sistema por agotamiento de recursos	Saturación del sistema informático	A8.6 Gestión de la capacidad	A
	R33	[A.3] Manipulación de los registros de actividad (log)	Alteración o eliminación de registros	A8.15 Registro	MB
	R35	[A.5] Suplantación de la identidad del usuario	Usurpación de derechos o privilegios	A5.16 Gestión de la identidad.	A
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R38	[A.8] Difusión de software dañino	Propagación intencionada de virus	A5.10 Uso aceptable de la información y otros activos asociados.	M
	R39	[A.9] [Re-]encaminamiento de mensajes	Desviación de mensajes que llega a un destino fraudulento	A8.20 Seguridad de redes	M
	R40	[A.10] Alteración de secuencia	modificación del orden de los datos para alterar el significado del mensaje	A8.16 Actividades de supervisión	M
	R42	[A.12] Análisis de tráfico	Ataque de análisis de tráfico para sacar para extraer información y hacer conclusiones	A8.16 Actividades de supervisión	M

	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R48	[A.22] Manipulación de programas	Alteración intencionada de los datos	A8.18 Uso de programas de utilidad privilegiados	A
	R50	[A.24] Denegación de servicio	Saturación del sistema informático	A8.20 Seguridad de redes	MA
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
Respaldo de información	R17	[E.2] Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación	A8.15 Registro.	A
	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R36	[A.6] Abuso de privilegios de acceso	Abuso de derechos	A8.18 Uso de programas de utilidad privilegiados	M
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros.	MA

				A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R52	[A.26] Ataque destructivo	Fallos deliberados causados por las personas, destrucción de Hardware	A8.21 Seguridad en los servicios de red A7.2 Entrada física A5.33 Protección de registros A5.15 Control de acceso	A
Inventario de Equipos y Licencias	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M
	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A

	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A
Información documental	R24	[E.15] Alteración accidental de la información	Alteración accidental de la información	A8.13 Copia de seguridad de la información.	M
	R25	[E.18] Destrucción de información	Eliminación intencional de información	A8.1 Dispositivos de punto final de usuario. A5.10 Uso aceptable de la información y otros activos asociados.	M
	R26	[E.19] Fugas de información	revelación de la información por indiscreción	A8.12 Prevención de fuga de datos.	MA
	R41	[A.11] Acceso no autorizado	Uso ilícito del hardware	A5.15 Control de acceso.	M

	R45	[A.15] Modificación deliberada de la información	Alteración intencional de la información	A8.32 Gestión del cambio.	A
	R46	[A.18] Destrucción de información	Pérdida accidental de información.	A5.33 Protección de registros. A6.3 Concienciación, educación y capacitación sobre seguridad de la información.	MA
	R47	[A.19] Divulgación de información	Copia ilegal de software	A8.3 Restricción de acceso a la información. A8.11 Enmascaramiento de datos.	MA
	R51	[A.25] Robo	Perdida de equipo provoca la indisponibilidad para presentar servicios	A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones. A8.24 Uso de criptografía.	A
	R4	[I.1] Fuego	Incendio, Posibilidad que el fuego acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	MA
	R5	[I.2] Daños por agua	Fuga o Inundaciones, Posibilidad que el agua acabe con recursos del sistema	A7.5 Protección contra amenazas físicas y ambientales.	A

Tratamiento del Riesgo

Evaluamos los riesgos de seguridad de la información, comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos y priorizar los riesgos analizados para el tratamiento de riesgos.

Determinamos todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información elegidas.

Anexo A contiene una lista de posibles controles de seguridad de la información, para garantizar que no se pasen por alto los controles necesarios de seguridad de la información. Los controles de seguridad de la información enumerados en el Anexo A no son exhaustivos y se pueden incluir controles de seguridad de la información adicionales si es necesario.

El Formular un plan de tratamiento de riesgos de seguridad de la información no está contemplado en el alcance, así que la cooperativa debe de definir cronológicamente como los atacará y mitigará. Además, debe de obtener la aprobación de los propietarios de riesgos del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información.

Según lo establecido por la norma ISO/IEC 27001, la organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

Las organizaciones sólo son conscientes de un porcentaje de todos sus riesgos. Puede ser que al finalizar se aprecie el esfuerzo realizado.

No todos los riesgos tienen el mismo origen, la cooperativa se debe de enfocar en los más importantes, los llamados riesgos no aceptables.

Existen cuatro opciones que puede escoger para **mitigar el riesgo no aceptable**.

- **Aplicar** controles de seguridad obtenidos del Anexo A para disminuir el riesgo; ejemplo: Realizar respaldo a la información crítica de la cooperativa.
- **Transferir** el riesgo a otras personas, ejemplo: Asegurando los activos de la cooperativa con una póliza de garantía con el proveedor.
- **Evitar** riesgos al detener la ejecución de la actividad que genera un elevado riesgo, o al hacerla de forma diferente; ejemplo: Cambiar el procedimiento de

ejecución de respaldo de la información a la base de datos modificando la configuración de respaldos completos a incrementales.

- **Aceptar el riesgo**, por ejemplo: si el **costo es mayor** o elevado al cambiar un sistema desfasado que se encuentra en producción, pero funcional, la cooperativa deberá tomar la decisión de asumir el riesgo de realizar el cambio de sistema.

Con el tratamiento de riesgo la cooperativa busca ser eficiente en la reducción y mitigación de riesgos críticos con la menor inversión.

Aplicabilidad de controles de ISO 27001

Los controles que aplicamos según los activos y riesgos en base al análisis realizado sobre los activos de la Cooperativa, donde identificamos las posibles amenazas que pudieran llegar a convertirse en riegos; proponemos la implementación de los siguientes controles de la norma IEC ISO 27001:2022 para proteger dichos activos de forma adecuada.

Tabla 3030 Controles ISO27001:2022

A5.10 Uso aceptable de la información y otros activos asociados
A5.15 Control de acceso
A5.16 Gestión de la identidad.
A5.33 Protección de registros
A6.3 Concienciación, educación y capacitación sobre seguridad de la información.
A6.4 Proceso disciplinario
A7.10 Medios de almacenamiento
A7.11 Utilidades de apoyo
A7.12 Seguridad del cableado
A7.13 Mantenimiento de equipos
A7.2 Entrada física
A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.
A7.5 Protección contra amenazas físicas y ambientales.
A8.1 Dispositivos de punto final de usuario.
A8.11 Enmascaramiento de datos.
A8.12 Prevención de fuga de datos.
A8.13 Copia de seguridad de la información.
A8.15 Registro
A8.16 Actividades de supervisión
A8.18 Uso de programas de utilidad privilegiados
A8.19 Instalación de software en sistemas operativos
A8.20 Seguridad de redes
A8.21 Seguridad en los servicios de red
A8.24 Uso de criptografía.
A8.25 Ciclo de vida de desarrollo seguro.
A8.29 Pruebas de seguridad en desarrollo y aceptación.
A8.3 Restricción de acceso a la información.
A8.32 Gestión del Cambio.
A8.5 Autenticación segura.
A8.6 Gestión de la capacidad
A8.7 Protección contra malware.
A8.9 Gestión de la configuración.

Diseño de requisitos de controles

A continuación, se detallan los controles que para la cooperativa SIHUACOOP se apegan a los activos identificados y analizados en la matriz de riesgo, estos llevarían a subsanarlos. Los siguientes puntos representan una guía que servirá a la cooperativa para determinar estrategias dentro su Plan de Tratamiento de riesgos para poder apegarse a la norma ISO 27001:2022 y más importante, proteger de forma adecuado los activos tangibles e intangibles, ya sean estos aplicaciones, datos, servicios o infraestructura.

A5.10 Uso aceptable de la información y otros activos asociados

Tabla 3131. Generalidades A5.10 Uso aceptable de la información y otros activos asociados

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
Preventivo	-Confidencialidad -Integridad -Disponibilidad	Proteger	-Gestión de Activos -Protección de la información	-Gobernanza y ecosistema -Protección

Control

Las normas de uso aceptable y los procedimientos de tratamiento de la información y otros activos asociados deben identificarse, documentarse y aplicarse.

Propósito

Garantizar que la información y otros activos asociados se protegen, utilizan y manejan adecuadamente.

Orientación

El personal y los usuarios externos que utilicen o tengan acceso a la información de la organización y otros activos asociados de la organización deben conocer los requisitos de seguridad de la información para proteger e información de la organización y otros activos asociados. Deben ser responsables de su uso de cualquier instalación de procesamiento de información.

La organización debe establecer una política específica sobre el uso aceptable de la información y otros activos asociados y comunicarla a todas las personas que utilicen o manejen la información y otros activos asociados. La política específica sobre el uso aceptable de la información debe proporcionar instrucciones claras sobre cómo se espera que las personas utilicen la información y otros activos asociados. La política específica del tema debe establecer:

a) los comportamientos esperados e inaceptables de las personas desde el punto de vista de la seguridad de la información<
b) uso permitido y prohibido de la información y otros activos asociados;
c) las actividades de control realizadas por la organización.

Los procedimientos de uso aceptable deben elaborarse para todo el ciclo de vida de la información de acuerdo con su clasificación y los riesgos determinados. Deben tenerse en cuenta los siguientes elementos:

1) restricciones de acceso que respalden los requisitos de protección de cada nivel de clasificación;
2) mantenimiento de un registro de los usuarios autorizados de la información y otros activos asociados;
3) protección de las copias temporales o permanentes de información a un nivel coherente con la protección de la información original;
4) almacenamiento de los activos asociados a la información de acuerdo con las especificaciones de los fabricantes;
5) marcado claro de todas las copias de los soportes de almacenamiento (electrónicos o físicos) a la atención del destinatario autorizado;
6) autorización de eliminación de la información y otros activos asociados;

Otra información.

Puede darse el caso de que los activos en cuestión no pertenezcan directamente a la organización, como los públicos en la nube. El uso de dichos activos de terceros y de cualquier activo de la organización asociado a dichos activos externos (por ejemplo, información, software) debe identificarse según proceda y controlarse, por ejemplo, mediante acuerdos con proveedores de servicios en la nube. También debe tenerse cuidado cuando se utilice un entorno de trabajo colaborativo.

A5.15 Control de acceso

Tabla 3232. Generalidades A5.15 Control de acceso.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
Preventivo	-Confidencialidad -Integridad -Disponibilidad	Proteger	-Gestión de identidad y acceso	-Protección

Control

Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse basándose en los requisitos de seguridad de la empresa y de la información.

Propósito

Garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Orientación

Los propietarios de la información y otros activos asociados deberían determinar los requisitos empresariales y de seguridad de la información relacionados con el control de acceso. Debería definirse una política temática específica sobre el control de acceso que tenga en cuenta estos requisitos y se comunique a todas las partes interesadas.

Estos requisitos y la política específica del tema deben considerar lo siguiente:

a) determinar qué entidades requieren qué tipo de acceso a la información y otros activos asociados;
b) seguridad de las aplicaciones;
c) acceso físico, que debe estar respaldado por controles físicos de entrada adecuados;
d) la difusión y autorización de la información (por ejemplo, el principio de necesidad de conocer) y la información niveles de seguridad y clasificación de la información;
e) restricciones al acceso privilegiado;
f) separación de funciones;
g) la legislación y los reglamentos pertinentes, así como cualquier obligación contractual relativa a la limitación del acceso a datos o servicios;
h) segregación de las funciones de control de acceso (por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso);
i) autorización formal de las solicitudes de acceso;
j) la gestión de los derechos de acceso;
k) logs o registros

Las normas de control de acceso deben aplicarse definiendo y asignando los derechos y restricciones de acceso adecuados a las entidades pertinentes. Una entidad puede representar

tanto a un usuario humano como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio). un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio). Para simplificar la gestión del control de acceso se pueden asignar funciones específicas a grupos de entidades.

A la hora de definir y aplicar las normas de control de acceso, debe tenerse en cuenta lo siguiente:

a) coherencia entre los derechos de acceso y la clasificación de la información;
b) coherencia entre los derechos de acceso y las necesidades y requisitos de seguridad del perímetro físico;
c) considerar todos los tipos de conexiones disponibles en entornos distribuidos, de modo que las entidades sólo tengan información y otros activos asociados, incluidas las redes y los servicios de red, que estén que estén autorizadas a utilizar;
d) considerar cómo pueden reflejarse los elementos o factores relevantes para el control de acceso dinámico.

Otra información.

A menudo se utilizan principios generales en el contexto del control de acceso. Dos de los principios más utilizados son:

a) necesidad de conocer: una entidad sólo tiene acceso a la información que necesita para realizar sus tareas (diferentes tareas o funciones implican diferentes necesidades de conocer la información y, por tanto, diferentes perfiles de acceso);
b) necesidad de uso: a una entidad sólo se le asigna acceso a la infraestructura de tecnología de la información cuando existe una necesidad clara;

A la hora de especificar las normas de control de acceso hay que tener cuidado:

a) establecer normas basadas en la premisa del menor privilegio, "Todo está generalmente prohibido a menos que expresamente permitido", en lugar de la norma más débil, "Todo está generalmente permitido a menos que expresamente prohibido";
b) los cambios en las etiquetas de información iniciados automáticamente por las y los iniciados a discreción de un usuario;
c) cambios en los permisos de usuario iniciados automáticamente por el sistema de información y aquellos iniciados por un administrador;
d) cuando definir y revisar periódicamente la aprobación.

Existen varias formas de aplicar el control de acceso, como MAC (control de acceso obligatorio), DAC (control de acceso discrecional), RBAC (control de acceso basado en roles) y ABAC (control de acceso basado en atributos).

Las reglas de control de acceso también pueden contener elementos dinámicos (por ejemplo, una función que evalúe accesos anteriores o valores específicos del entorno). Las reglas de control de acceso pueden aplicarse con distintos grados de granularidad, desde redes o sistemas enteros hasta campos de datos específicos, y también pueden tener en cuenta propiedades como la ubicación del usuario o el tipo de conexión de red que se utiliza para el acceso. Estos principios y granularidad del control de acceso pueden tener un impacto significativo en los costes. Unas normas más estrictas y una mayor granularidad suelen conllevar un coste más elevado. Los requisitos empresariales y las consideraciones de riesgo deben utilizarse para definir qué reglas de control de acceso se aplican y qué granularidad se requiere.

A5.16 Gestión de la identidad.

Tabla 3333. Generalidades A5.16 Gestión de la identidad.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
Preventivo	-Confidencialidad -Integridad -Disponibilidad	Proteger	-Gestión de identidad y acceso	-Protección

Controlar

Debe gestionarse el ciclo de vida completo de las identidades.

Propósito

Permitir la identificación única de los individuos y sistemas que acceden a la información de la organización y a otros activos asociados, y permitir la asignación adecuada de derechos de acceso.

Orientación

Los procesos utilizados en el contexto de la gestión de identidades deben garantizar que:

a) en el caso de las identidades asignadas a personas, una identidad específica sólo se vincula a una única persona para poder responsabilizar a la persona de las acciones realizadas con esta identidad específica;
b) las identidades asignadas a varias personas (por ejemplo, las identidades compartidas) sólo se permitirán cuando sean necesarias por razones empresariales u operativas y estén sujetas a aprobación y documentación específicas;
c) las identidades asignadas a entidades no humanas están sujetas a una aprobación debidamente segregada y a una supervisión continua independiente;
d) las identidades se desactiven o eliminen en el momento oportuno si ya no son necesarias (por ejemplo, si sus entidades asociadas se eliminan o ya no se utilizan, o si la persona vinculada a una identidad ha abandonado la organización o ha cambiado de función);
e) en un ámbito específico, se asigna una única identidad a una única entidad, [es decir, se evita la asignación de múltiples identidades a la misma entidad dentro del mismo contexto (identidades duplicadas)];
f) se mantengan registros de todos los eventos significativos relacionados con el uso y la gestión de las identidades de usuario y de la información de autenticación.

La organización debe disponer de un proceso de apoyo para gestionar los cambios en la información relacionada con las identidades de los usuarios. Estos procesos pueden incluir la nueva verificación de los documentos de confianza relacionados con una persona.

Cuando se utilizan identidades proporcionadas o emitidas por terceros (por ejemplo, credenciales de redes sociales), la organización debe asegurarse de que las identidades de terceros proporcionan el nivel de confianza requerido y de que cualquier riesgo asociado se conoce y se trata suficientemente. Esto puede incluir controles relacionados con los terceros, así como controles relacionados con la información de autenticación asociada.

Otra información

Proporcionar o revocar el acceso a la información y a otros activos asociados suele ser un procedimiento que consta de varios pasos:

a) confirmar los requisitos de negocio para que se establezca una identidad;

b) verificar la identidad de una entidad antes de asignarle una identidad lógica;

c) establecimiento de una identidad

d) configuración y activación de la identidad. Esto incluye también la configuración y el establecimiento inicial de servicios de autenticación;

e) conceder o revocar derechos de acceso específicos a la identidad, basándose en las decisiones de autorización o decisiones sobre derechos.

A5.33 Protección de registros

Tabla 3434. Generalidades A5.33 Protección de registros.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Identificar -Proteger	-Legal y cumplimiento -Gestión de activos -Protección de la información	-Defensa

Controlar

Los registros deben protegerse de la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.

Propósito

Garantizar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales, así como las expectativas de la comunidad o la sociedad en relación con la protección y disponibilidad de los documentos de archivo.

Orientación

La organización debe adoptar las siguientes medidas para proteger la autenticidad, fiabilidad, integridad y usabilidad de los documentos de archivo, a medida que cambien con el tiempo su contexto empresarial y los requisitos para su gestión:

a) emitir directrices sobre el almacenamiento, la manipulación, la cadena de custodia y la eliminación de los registros, lo que incluye prevención de la manipulación de los registros. Estas directrices deben estar en consonancia con la política de la organización política específica de la organización en materia de gestión de documentos y otros requisitos relativos a los documentos;
b) elaborar un calendario de conservación en el que se definan los registros y el periodo de tiempo durante el cual deben conservarse.

El sistema de almacenamiento y manipulación debe garantizar la identificación de los registros y de su período de conservación, teniendo en cuenta la legislación o la normativa nacional o regional, así como las expectativas comunidad o la sociedad, si procede. Este sistema debe permitir la destrucción adecuada de los documentos de ese periodo si la organización no los necesita.

A la hora de decidir sobre la protección de determinados registros de la organización, debe tenerse en cuenta su correspondiente clasificación de seguridad de la información, basada en el esquema de clasificación de la organización. Los registros deben clasificarse en tipos de registro (por ejemplo, registros contables, registros de transacciones comerciales, registros de personal,

registros legales), cada uno con detalles sobre los periodos de conservación y el tipo de medio de almacenamiento permitido, que puede ser físico o electrónico.

Los sistemas de almacenamiento de datos deben elegirse de forma que los registros necesarios puedan recuperarse en un plazo y formato aceptables, en función de los requisitos que deban cumplirse.

Si se opta por medios de almacenamiento electrónicos, deben establecerse procedimientos que garanticen la capacidad de acceso a los documentos de archivo (tanto a los medios de almacenamiento como a la legibilidad del formato) durante todo el periodo de conservación, a fin de evitar pérdidas debidas a futuros cambios tecnológicos. También deben conservarse las claves criptográficas y los programas asociados a los archivos cifrados o a las firmas digitales para permitir el descifrado de los documentos durante el periodo de conservación.

Los procedimientos de almacenamiento y manipulación deben aplicarse de acuerdo con las recomendaciones de los fabricantes de los medios de almacenamiento. Debe tenerse en cuenta la posibilidad de deterioro de los soportes utilizados para almacenar los documentos.

Otra información

Los registros documentan eventos o transacciones individuales o pueden formar agregaciones que han sido diseñadas para documentar procesos de trabajo, actividades o funciones. Son a la vez pruebas de la actividad empresarial y activos de información. Cualquier conjunto de información, independientemente de su estructura o forma, puede gestionarse como un registro. Esto incluye la información en forma de documento, una colección de datos u otros tipos de información digital o analógica que se crean, procesan o almacenan. digital o analógica que se crea, captura y gestiona en el transcurso de la actividad empresarial.

En la gestión de documentos de archivo, los metadatos son datos que describen el contexto, el contenido y la estructura de los documentos de archivo, así como su gestión a lo largo del tiempo. Los metadatos son un componente esencial de cualquier documento de archivo.

Puede ser necesario conservar algunos documentos de forma segura para cumplir requisitos legales, reglamentarios o contractuales, así como para respaldar actividades empresariales esenciales. Las leyes o normativas nacionales pueden establecer el periodo de tiempo y el contenido de los datos para la conservación de la información.

A6.3 Concienciación, educación y capacitación sobre seguridad de la información.

Tabla 3535. Generalidades A6.3 Concienciación, educación y capacitación sobre seguridad de la información.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Identificar -Proteger	-Legal y cumplimiento -Protección de la información	-Protección

Control

La organización debería identificar y cumplir los requisitos relativos a la preservación de la privacidad y protección de PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

Propósito

Para asegurar el cumplimiento de los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con los aspectos de seguridad de la información de la protección de PII.

Orientación

Se debe establecer un programa de concientización, educación y capacitación en seguridad de la información en línea con la política de seguridad de la información de la organización, las políticas específicas del tema y los procedimientos relevantes en seguridad de la información, tomando en consideración la información de la organización a proteger y los controles de seguridad de la información que se han implementado para proteger la información.

La concientización, la educación y la capacitación en seguridad de la información deben llevarse a cabo periódicamente. Inicialmente la concientización, la educación y la capacitación pueden aplicarse al personal nuevo y a aquellos que se transfieren a nuevos puestos o roles con requisitos de seguridad de la información sustancialmente diferentes.

La comprensión del personal debe evaluarse al final de una actividad de sensibilización, educación o formación para probar la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y formación.

Conciencia

Un programa de concientización sobre la seguridad de la información debe apuntar a que el personal sea consciente de sus responsabilidades para la seguridad de la información y los medios por los cuales se cumplen esas responsabilidades.
El programa de sensibilización debe planificarse teniendo en cuenta las funciones del personal en la organización, incluido el personal interno y externo (por ejemplo, consultores externos, personal del proveedor).

Las actividades del programa de concientización deben programarse a lo largo del tiempo, preferiblemente con regularidad, de modo que las actividades se repitan y cubran personal nuevo. También debe basarse en las lecciones aprendidas de incidentes de seguridad de la información.
El programa de sensibilización debe incluir una serie de actividades de sensibilización a través de canales físicos o virtuales como campañas, folletos, carteles, boletines, sitios web, información sesiones, sesiones informativas, módulos de aprendizaje electrónico y correos electrónicos.

La concientización sobre la seguridad de la información debe cubrir aspectos generales tales como:

a) el compromiso de la dirección con la seguridad de la información en toda la organización;
b) las necesidades de familiaridad y cumplimiento con respecto a las normas y obligaciones de seguridad de la información aplicables, teniendo en cuenta la política de seguridad de la información y las políticas, estándares, leyes, estatutos, reglamentos, contratos y convenios;
c) responsabilidad personal por las propias acciones e inacciones, y responsabilidades generales hacia asegurar o proteger la información perteneciente a la organización y las partes interesadas;
d) procedimientos básicos de seguridad de la información [por ejemplo: informes de eventos de seguridad de la información y referencia controles [por ejemplo: seguridad de contraseña.
e) puntos de contacto y recursos para información adicional y asesoramiento sobre seguridad de la información asuntos, incluidos más materiales de concientización sobre la seguridad de la información.

Educación y entrenamiento

La organización debe identificar, preparar e implementar un plan de capacitación adecuado para los equipos cuyas funciones requieren conjuntos de habilidades y experiencia específicos. Los equipos técnicos deben tener las habilidades para configurar y mantener el nivel de seguridad requerido para dispositivos, sistemas, aplicaciones y servicios. Si faltan habilidades, la organización debe tomar medidas y adquirirlas.

El programa de educación y capacitación debe considerar diferentes formas [p. conferencias o autoestudios, ser asesorado por personal experto o consultores (capacitación en el trabajo), rotar a los miembros del personal para seguir diferentes actividades, reclutando personas ya calificadas y contratando consultores]. Puede utilizar diferentes medios. de la entrega, incluido el aprendizaje en el aula, a distancia, basado en la web, a su propio ritmo y otros. Técnico El personal debe mantener sus conocimientos actualizados suscribiéndose a boletines y revistas o asistir a congresos y eventos destinados a la mejora técnica y profesional.

A6.4 Proceso disciplinario

Tabla 3636. Generalidades A6.4 Proceso disciplinario.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Correctivo	-Confidencialidad -Integridad -Disponibilidad	-Identificar -Proteger	-Responder. -Proteger. -Recursos Humanos	-Gobernanza y Ecosistema

Control

Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

Objetivo.

Asegurar que el personal y otras partes interesadas entiendan las consecuencias de la violación de la política de seguridad de información, para disuadir y tratar adecuadamente al personal y otras partes interesadas relevantes que cometieron la velación.

Guía de Orientación.

El proceso disciplinario no debe iniciarse sin la verificación previa de que un responsable de seguridad de la información ha ocurrido una violación de la política.

El proceso disciplinario formal debe prever una respuesta graduada que tenga en cuenta factores tales como:

a) la naturaleza (quién, qué, cuándo, cómo) y la gravedad del incumplimiento y sus consecuencias;
b) si el delito fue intencional (malicioso) o no intencional (accidental);
c) si se trata o no de una primera o reiterada infracción;
d) si el infractor fue debidamente capacitado o no.

La respuesta debe tener en cuenta las disposiciones legales, estatutarias, reglamentarias, contractuales y requisitos comerciales, así como otros factores según sea necesario. El proceso disciplinario también debe ser utilizado como un elemento disuasorio para evitar que el personal y otras partes interesadas relevantes violen la política de seguridad de la información, políticas y procedimientos específicos del tema para la seguridad de la información. Las violaciones de la política de seguridad de la información pueden requerir acciones inmediatas.

Información adicional.

Siempre que sea posible, la identidad de las personas sujetas a medidas disciplinarias debe protegerse de conformidad con los requisitos aplicables. Cuando las personas demuestran un comportamiento excelente en materia de seguridad de la información, pueden ser recompensados para promover la seguridad de la información y fomentar el buen comportamiento.

A7.10 Medios de almacenamiento

Tabla 3737. Generalidades A7.10 Medios de almacenamiento.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad Física -Gestión de Activos	-Protección

Control

Los soportes de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.

Propósito

Garantizar que sólo se autoriza la divulgación, modificación, eliminación o destrucción de información en soportes de almacenamiento. almacenamiento.

Orientación

Soportes de almacenamiento extraíbles

Deben tenerse en cuenta las siguientes directrices para la gestión de soportes de almacenamiento extraíbles:

a) establecer una política temática específica sobre la gestión de soportes de almacenamiento extraíbles y comunicar dicha política a cualquier persona que utilice o manipule soportes de almacenamiento extraíbles;
b) cuando sea necesario y práctico, exigir autorización para retirar los soportes de almacenamiento de la organización y mantener un registro de dichas retiradas con el fin de conservar una pista de auditoría;
c) almacenar todos los soportes de almacenamiento en un entorno seguro de acuerdo con su clasificación de la información y protegiéndolos contra las amenazas medioambientales (como el calor, la humedad, el electrónico o envejecimiento), de acuerdo con las especificaciones de los fabricantes;

d) si la confidencialidad o la integridad de la información son consideraciones importantes, utilizar técnicas criptográficas para proteger la información en soportes de almacenamiento extraíbles;
e) para mitigar el riesgo de que los soportes de almacenamiento se degraden mientras la información almacenada sigue siendo necesaria, transferir la información a medios de almacenamiento nuevos antes de que sea ilegible;
f) almacenar múltiples copias de información valiosa en soportes de almacenamiento separados para reducir aún más el riesgo de daños o pérdidas de información accidentales;
g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;
h) habilitar puertos de medios de almacenamiento extraíbles [por ejemplo, ranuras para tarjetas digitales seguras (SD) y puertos de bus serie universal (USB)] únicamente si existe una razón organizativa para su uso;
i) cuando sea necesario utilizar medios de almacenamiento extraíbles, supervisar la transferencia de información a dichos medios de almacenamiento;
j) la información puede ser vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico, por ejemplo, cuando se envían soportes de almacenamiento a través del servicio postal o de mensajería.

En este control, los soportes incluyen los documentos en papel. Al transferir soportes físicos de almacenamiento, aplique medidas de seguridad.

Reutilización o eliminación seguras

Deben establecerse procedimientos para la reutilización o eliminación segura de los soportes de almacenamiento con el fin de minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Los procedimientos para la reutilización o eliminación segura de soportes de almacenamiento que contengan información confidencial deben ser proporcionales a la sensibilidad de dicha información. Deberán tenerse en cuenta los siguientes aspectos:

a) si es necesario reutilizar dentro de la organización soportes de almacenamiento que contengan información confidencial, eliminar de forma segura los datos o formatear el soporte de almacenamiento antes de reutilizarlo;
b) eliminar de forma segura los soportes de almacenamiento que contengan información confidencial cuando ya no se necesiten (por ejemplo, destruyendo, triturando o borrando de forma segura el contenido);
c) disponer de procedimientos para identificar los elementos que pueden requerir una eliminación segura;
d) muchas organizaciones ofrecen servicios de recogida y eliminación de soportes de almacenamiento. Hay que tener cuidado a la hora de seleccionar un proveedor externo adecuado que cuente con los controles y la experiencia adecuados;
e) registrar la eliminación de artículos sensibles para mantener una pista de auditoría;
f) al acumular soportes de almacenamiento para su eliminación, tener en cuenta el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se convierta en sensible. Debe realizarse una evaluación de riesgos de los dispositivos dañados que contengan datos sensibles para determinar si los elementos deben destruirse físicamente en lugar de enviarlos a reparar o desecharlos.

Otra información

Cuando la información confidencial de los soportes de almacenamiento no está cifrada, debe considerarse la posibilidad de proteger físicamente los soportes de almacenamiento.

A7.11 Utilidades de apoyo.

Tabla 3838. Generalidades A7.11 Utilidades de apoyo.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Detectar	-Confidencialidad -Integridad -Disponibilidad	-Proteger -Detectar	-Seguridad Física	-Protección

Control.

Las instalaciones de procesamiento de información deben protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

Objetivo.

Para evitar la pérdida, el daño o el compromiso de la información y otros activos asociados, o la interrupción de las operaciones de la organización debido a fallas e interrupciones de los servicios públicos de apoyo.

Orientación.

Las organizaciones dependen de los servicios públicos (ejemplo: electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado) para respaldar sus instalaciones de procesamiento de información. Por lo tanto, la organización debe:

a) asegurar que el equipo de apoyo a los servicios públicos esté configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente;
b) garantizar que las empresas de servicios públicos sean evaluadas regularmente por su capacidad para satisfacer el crecimiento y las interacciones comerciales con otras utilidades de apoyo;
c) asegurarse de que el equipo de apoyo a los servicios públicos se inspeccione y pruebe regularmente para garantizar su correcto funcionamiento marcha;

d) si es necesario, activar alarmas para detectar fallas en los servicios públicos;
e) si es necesario, asegúrese de que las empresas de servicios públicos tengan múltiples alimentaciones con diversas rutas físicas;
f) asegurarse de que el equipo de apoyo a los servicios públicos esté en una red separada del procesamiento de información instalaciones si está conectado a una red;
g) asegurarse de que el equipo de apoyo a los servicios públicos esté conectado a Internet solo cuando sea necesario y solo de manera segura.

Se debe proporcionar iluminación de emergencia y comunicaciones. Interruptores de emergencia y válvulas para cortar. Los cortes de energía, agua, gas u otros servicios públicos deben ubicarse cerca de las salidas de emergencia o las salas de equipos. Los detalles de contacto de emergencia deben registrarse y estar disponibles para el personal en caso de una interrupción.

Otra información

Se puede obtener redundancia adicional para conectividad de red mediante múltiples rutas desde más de un proveedor de servicios públicos.

A7.12 Seguridad del cableado

Tabla 3939. Generalidades A7.12 Seguridad del cableado.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Disponibilidad	-Proteger	-Seguridad Física	-Protección

Control

Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra intercepciones, interferencia o daño.

Propósito

Para evitar la pérdida, el daño, el robo o el compromiso de la información y otros activos asociados e interrupción de las operaciones de la organización relacionadas con el cableado de energía y comunicaciones.

Orientación

Se deben considerar las siguientes pautas para la seguridad del cableado:

a) las líneas eléctricas y de telecomunicaciones a las instalaciones de procesamiento de información son subterráneas donde sea posible, o sujeto a una protección alternativa adecuada, como protector de cable de piso y poste de electricidad; si los cables son subterráneos, protegerlos de cortes accidentales (por ejemplo, con armaduras) conductos o señales de presencia);

b) separar los cables de alimentación de los cables de comunicaciones para evitar interferencias;

c) para sistemas sensibles o críticos, los controles adicionales a considerar incluyen:

1) instalación de conductos blindados y cuartos o cajas cerradas y alarmas en inspección y puntos de terminación;

2) uso de blindaje electromagnético para proteger los cables;

3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados unido a los cables;

4) acceso controlado a paneles de conexión y salas de cables (p. ej., con llaves mecánicas o PIN);

5) uso de cables de fibra óptica;

d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación e inspección del cable.

Se debe buscar el asesoramiento de especialistas sobre cómo gestionar los riesgos derivados de incidentes de cableado o fallos de funcionamiento

Otra información.

A veces, el cableado de energía y telecomunicaciones son recursos compartidos por más de una organización ocupando locales compartidos.

A7.13 Mantenimiento de equipos

Tabla 4040. Generalidades A7.13 Mantenimiento de equipos.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad Física -Gestión de Activos	-Protección -Resiliencia

Controlar

Los equipos deben mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

Propósito

Evitar la pérdida, el daño, el robo o la puesta en peligro de la información y otros activos asociados, así como la interrupción de las operaciones de la organización causada por la falta de mantenimiento.

Orientación

Deben tenerse en cuenta las siguientes directrices para el mantenimiento de los equipos:

a) mantener los equipos de acuerdo con la frecuencia de servicio y las especificaciones recomendadas por el proveedor;
b) aplicación y supervisión de un programa de mantenimiento por parte de la organización;
c) que sólo el personal de mantenimiento autorizado lleve a cabo las reparaciones y el mantenimiento de los equipos
d) mantenimiento de registros de todas las averías presuntas o reales y de todo el mantenimiento preventivo y correctivo;
e) la aplicación de controles adecuados cuando se programe el mantenimiento de los equipos, teniendo en cuenta si este mantenimiento lo realiza personal in situ o externo a la organización; sometiendo al personal de mantenimiento a un acuerdo de confidencialidad adecuado;
f) supervisar al personal de mantenimiento cuando realice tareas de mantenimiento en sitio;
g) autorizar y controlar el acceso para el mantenimiento a distancia;
h) aplicar medidas de seguridad para los activos fuera de los locales si los equipos que contienen información se sacan de los locales para su mantenimiento;
i) cumplir todos los requisitos de mantenimiento impuestos por los seguros
j) antes de volver a poner en funcionamiento los equipos tras su mantenimiento, inspeccionarlos para garantizar que no han sido manipulados y que funcionan correctamente;
k) aplicar medidas para la eliminación segura o la reutilización de los equipos si se determina que deben eliminarse.

Otra información

Los equipos incluyen los componentes técnicos de las instalaciones de tratamiento de la información, sistemas de alimentación ininterrumpida (SAI) y baterías, generadores de energía, alternadores y convertidores de energía, sistemas de detección de intrusión física y alarmas, detectores de humo, extintores, aire acondicionado y ascensores.

A7.2 Entrada física

Tabla 4141. Generalidades A7.2 Entrada física.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad Física -Gestión de identidad y de acceso	-Protección

Controlar

Las zonas seguras deben protegerse mediante controles de entrada y puntos de acceso adecuados.

Propósito

Garantizar que sólo se produce el acceso físico autorizado a la información de la organización y a otros activos asociados.

Orientación

General

Los puntos de acceso, como las zonas de entrega y carga y otros puntos en los que pueden entrar personas no autorizadas, deben controlarse y, si es posible, aislarse de las instalaciones de procesamiento de la información para evitar accesos no autorizados.

Deberán tenerse en cuenta las siguientes directrices:

a) restringir el acceso a las instalaciones y edificios únicamente al personal autorizado. El proceso de gestión de los derechos de acceso a las áreas físicas debe incluir la provisión, revisión periódica, actualización y revocación de las autorizaciones;
b) mantener y supervisar de forma segura un libro de registro físico o una pista de auditoría electrónica de todos los accesos y proteger todos los registros y la información sensible de autenticación;
c) establecer y aplicar un proceso y mecanismos técnicos para la gestión del acceso a las zonas en las que se procesa o almacena información. Los mecanismos de autenticación incluyen el uso de tarjetas de acceso, biometría o autenticación de dos factores, como una tarjeta de acceso y un PIN secreto. Para el acceso a las zonas sensibles debe considerarse la posibilidad de utilizar puertas de doble seguridad;
d) establecimiento de una zona de recepción vigilada por personal, u otros medios para controlar el acceso físico al lugar o edificio
e) inspeccionar y examinar los efectos personales del personal y las partes interesadas a la entrada y a la salida;

NOTA Puede existir legislación y normativa local sobre la posibilidad de inspeccionar los efectos personales.

f) exigir a todo el personal y a las partes interesadas que lleven algún tipo de identificación visible y que avisen inmediatamente al personal de seguridad si se encuentran con visitantes sin escolta y con cualquier persona que no lleve una identificación visible. Para identificar mejor a los empleados fijos, los proveedores y los visitantes, debería considerarse la posibilidad de utilizar distintivos fácilmente distinguibles;
g) conceder al personal de los proveedores un acceso restringido a las zonas seguras o a las instalaciones de tratamiento de la información sólo cuando sea necesario. Este acceso debe ser autorizado y supervisado;
h) prestar especial atención a la seguridad del acceso físico en el caso de edificios que alberguen activos para múltiples organizaciones;
i) diseñar las medidas de seguridad física de modo que puedan reforzarse cuando aumente la probabilidad de incidentes físicos;
j) proteger otros puntos de entrada, como las salidas de emergencia, de accesos no autorizados;
k) establecer un proceso de gestión de llaves que garantice la gestión de las llaves físicas o la información de autenticación (por ejemplo, códigos de cerraduras, cerraduras de combinación de oficinas, salas e instalaciones como armarios de llaves) y que garantice un libro de registro o una auditoría anual de llaves y que se controle el acceso a las llaves físicas o a la información de autenticación.

Visitantes

Deben tenerse en cuenta las siguientes directrices:

a) autenticar la identidad de los visitantes por un medio adecuado;
b) registrar la fecha y hora de entrada y salida de los visitantes
c) conceder acceso a los visitantes únicamente para fines específicos y autorizados, y con instrucciones sobre los requisitos de seguridad de la zona y sobre los procedimientos de emergencia;
d) supervisar a todos los visitantes, a menos que se conceda una excepción explícita.

Zonas de entrega de carga y material entrante

Deberán tenerse en cuenta las siguientes directrices

a) restringir el acceso a las zonas de entrega y carga desde el exterior del edificio al personal identificado y autorizado;
b) diseñar las zonas de entrega y carga de forma que las entregas puedan cargarse y descargarse sin que el personal de entrega acceda sin autorización a otras partes del edificio;
c) asegurar las puertas exteriores de las zonas de entrega y carga cuando se abran las puertas de las zonas restringidas
d) inspeccionar y examinar las entregas entrantes en busca de explosivos, productos químicos u otros materiales peligrosos antes de que salgan de las zonas de entrega y carga;
e) registrar las entregas entrantes de acuerdo con los procedimientos de gestión de activos a la entrada en las instalaciones

f) separar físicamente los envíos entrantes y salientes, siempre que sea posible
g) inspeccionar las entregas entrantes en busca de indicios de manipulación en el camino. Si se descubren manipulaciones, deben comunicarse inmediatamente al personal de seguridad.

A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.

Tabla 4242. Generalidades A7.3 Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad Física -Gestión de Activos	-Protección

Controlar

Se debe diseñar e implementar la seguridad física de oficinas, salas e instalaciones.

Propósito

Impedir el acceso físico no autorizado, el daño y la interferencia en la información de la organización y otros activos asociados en oficinas, salas e instalaciones.

Orientación

Deben tenerse en cuenta las siguientes directrices para proteger oficinas, salas e instalaciones:

1. ubicar las instalaciones críticas para evitar el acceso del público;
2. cuando proceda, velar por que los edificios sean discretos y den una indicación mínima de su finalidad, sin signos evidentes, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de la información;
3. configurar las instalaciones para evitar que la información o las actividades confidenciales sean visibles y audibles desde el exterior. También deberá considerarse, en su caso, el blindaje electromagnético;
4. no poner a disposición de cualquier persona no autorizada directorios, guías telefónicas internas y mapas accesibles en línea que identifiquen la ubicación de las instalaciones de tratamiento de información confidencial.

A7.5 Protección contra amenazas físicas y ambientales.

Tabla 4343. Generalidades A7.5 Protección contra amenazas físicas y ambientales.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad Física	-Protección

Controlar

Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.

Propósito

Prevenir o reducir las consecuencias de sucesos originados por amenazas físicas y medioambientales.

Orientación

Las evaluaciones de riesgos para identificar las consecuencias potenciales de las amenazas físicas y medioambientales deben realizarse antes de comenzar las operaciones críticas en un emplazamiento físico, y a intervalos regulares. Deben aplicarse las salvaguardias necesarias y vigilarse los cambios que se produzcan en las amenazas. Debe obtenerse asesoramiento especializado sobre cómo gestionar los riesgos derivados de amenazas físicas y medioambientales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y otras formas de catástrofes naturales o provocadas por el ser humano.

La ubicación física de los locales y su construcción deben tener en cuenta

a) la topografía local, como la elevación adecuada, las masas de agua y las fallas tectónicas;
b) las amenazas urbanas, como los lugares con un perfil elevado para atraer disturbios políticos, actividades delictivas o atentados terroristas.

Basándose en los resultados de la evaluación de riesgos, deben identificarse las amenazas físicas y medioambientales pertinentes y considerarse los controles adecuados en los siguientes contextos, a modo de ejemplo:

a) incendio: instalación y configuración de sistemas capaces de detectar incendios en una fase temprana para enviar alarmas o activar sistemas de extinción de incendios con el fin de evitar daños por incendio a los soportes de almacenamiento y a los sistemas de tratamiento de la información relacionados. La extinción de incendios debe realizarse utilizando la sustancia más adecuada en relación con el entorno circundante (por ejemplo, gas en espacios confinados);

b) inundación: instalación de sistemas capaces de detectar inundaciones en una fase temprana bajo los suelos de las zonas que contengan soportes de almacenamiento o sistemas de tratamiento de la información. En caso de inundación, deberá disponerse de bombas de agua o medios equivalentes;
c) sobretensiones eléctricas: adopción de sistemas capaces de proteger los sistemas de información tanto de los servidores como de los clientes contra sobretensiones eléctricas o sucesos similares para minimizar las consecuencias de tales sucesos;
d) explosivos y armas: realizar inspecciones aleatorias para detectar la presencia de explosivos o armas en el personal, los vehículos o los bienes que entren en las instalaciones de tratamiento de información sensible.

Otra información

Las cajas fuertes u otras formas de instalaciones de almacenamiento seguro pueden proteger la información almacenada en ellas contra catástrofes como incendios, terremotos, inundaciones o explosiones.

Las organizaciones pueden tener en cuenta los conceptos de prevención de la delincuencia mediante el diseño medioambiental a la hora de diseñar los controles para asegurar su entorno y reducir las amenazas urbanas. Por ejemplo, en lugar de utilizar bolardos, las estatuas o elementos acuáticos pueden servir a la vez de elemento y de barrera física.

A8.1 Dispositivos de punto final de usuario.

Tabla 4444. Generalidades A8.1 Dispositivos de punto final de usuario.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Gestión de activos -Protección de la información	-Protección

Controlar

Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.

Propósito

Proteger la información contra los riesgos introducidos por el uso de dispositivos de punto final de usuario.

Orientación

General

La organización debe establecer una política específica sobre la configuración y el manejo seguros de los dispositivos de punto final de usuario. La política específica del tema debe ser comunicada a todo el personal relevante y considerar lo siguiente:

a) el tipo de información y el nivel de clasificación que los dispositivos de punto final de usuario pueden manejar, procesar, almacenar o admitir;
b) el registro de los dispositivos de punto final de usuario
c) requisitos de protección física
d) restricción de la instalación de software (por ejemplo, controlado a distancia por los administradores del sistema)
e) requisitos para el software de los dispositivos de punto final de usuario (incluidas las versiones de software) y para la aplicación de actualizaciones (por ejemplo, actualización automática activa)
f) normas para la conexión a servicios de información, redes públicas o cualquier otra red fuera de las instalaciones (por ejemplo, exigiendo el uso de un cortafuegos personal)
g) controles de acceso
h) cifrado de dispositivos de almacenamiento
i) protección contra programas maliciosos
j) desactivación, supresión o bloqueo a distancia;
k) copias de seguridad;

l) uso de servicios y aplicaciones web;
m) análisis del comportamiento del usuario final;
n) el uso de dispositivos extraíbles, incluidos los dispositivos de memoria extraíbles, y la posibilidad de desactivar puertos físicos (por ejemplo, puertos USB);
o) el uso de capacidades de partición, si son compatibles con el dispositivo de punto final del usuario, que pueden separar de forma segura la información de la organización y otros activos asociados (por ejemplo, software) de otra información y otros activos asociados en el dispositivo.

Debe considerarse si cierta información es tan sensible que sólo puede accederse a ella a través de dispositivos de punto final de usuario, pero no almacenarse en dichos dispositivos. En tales casos, pueden exigirse salvaguardias técnicas adicionales en el dispositivo. Por ejemplo, garantizar que la descarga de archivos para trabajar sin conexión esté desactivada y que el almacenamiento local, como la tarjeta SD, esté desactivado.

En la medida de lo posible, las recomendaciones sobre este control deben aplicarse mediante la gestión de la configuración o herramientas automatizadas.

Responsabilidad de los usuarios

Todos los usuarios deben conocer los requisitos y procedimientos de seguridad para proteger los dispositivos de punto final de los usuarios, así como sus responsabilidades a la hora de aplicar dichas medidas de seguridad. Se debe aconsejar a los usuarios que:

a) cerrar las sesiones activas y finalizar los servicios cuando ya no los necesiten;
b) proteger los dispositivos de punto final del usuario contra el uso no autorizado mediante un control físico (por ejemplo, cerradura con llave o cerraduras especiales) y un control lógico (por ejemplo, acceso mediante contraseña) cuando no estén en uso; no dejar desatendidos los dispositivos que contengan información importante, sensible o crítica para la empresa;
c) utilizar los dispositivos con especial cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras zonas no protegidas (por ejemplo, evitar leer información confidencial si la gente puede leer por detrás, utilizar filtros de privacidad en la pantalla);
d) proteger físicamente los dispositivos de punto final de los usuarios contra robos (por ejemplo, en coches y otros medios de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

Debe establecerse un procedimiento específico que tenga en cuenta los requisitos legales, estatutarios, reglamentarios, contractuales (incluido el seguro) y otros requisitos de seguridad de la organización para los casos de robo o pérdida de dispositivos de punto final de usuario.

Uso de dispositivos personales

Cuando la organización permita el uso de dispositivos personales (a veces conocido como BYOD), además de las orientaciones dadas en este control, se debe tener en cuenta lo siguiente:

a) la separación del uso personal y empresarial de los dispositivos, incluido el uso de software para respaldar dicha separación y proteger los datos empresariales en un dispositivo privado;
b) proporcionar acceso a la información empresarial sólo después de que los usuarios hayan reconocido sus obligaciones (protección física, actualización del software, etc.), renunciar

a la propiedad de los datos empresariales, permitir el borrado remoto de los datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no se esté autorizado a utilizar el servicio. En estos casos, debe tenerse en cuenta la legislación sobre protección de la IPI;

c) políticas y procedimientos específicos por temas para evitar disputas sobre derechos de propiedad intelectual desarrollados en equipos de propiedad privada;
d) el acceso a equipos de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), que puede impedirse mediante legislación;
e) acuerdos de licencia de software que puedan hacer a las organizaciones responsables de las licencias de software de cliente en dispositivos de punto final de propiedad privada del personal o de usuarios externos.

Conexiones inalámbricas

La organización debe establecer procedimientos para:

a) la configuración de las conexiones inalámbricas en los dispositivos (por ejemplo, desactivando los protocolos vulnerables);
b) el uso de conexiones inalámbricas o por cable con un ancho de banda adecuado de acuerdo con las políticas específicas de cada tema (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de software).

Otra información

Los controles para proteger la información de los dispositivos de punto final de usuario dependen de si el dispositivo de punto final de usuario se utiliza únicamente dentro de las instalaciones y conexiones de red seguras de la organización, o si está expuesto a mayores amenazas físicas y relacionadas con la red fuera de la organización.

Las conexiones inalámbricas para dispositivos de punto final de usuario son similares a otros tipos de conexiones de red, pero presentan diferencias importantes que deben tenerse en cuenta a la hora de identificar los controles. En particular, las copias de seguridad de la información almacenada en los dispositivos de punto final de usuario pueden fallar a veces debido al ancho de banda limitado de la red o porque los dispositivos de punto final de usuario no están conectados en los momentos en que están programadas las copias de seguridad.

En el caso de algunos puertos USB, como el USB-C, no es posible desactivar el puerto USB porque se utiliza para otros fines (por ejemplo, suministro de energía y salida de pantalla).

A8.11 Enmascaramiento de datos.

Tabla 4545. Generalidades A8.11 Enmascaramiento de datos.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad	-Proteger	-Protección de la información	-Protección

Control

El enmascaramiento de datos debe utilizarse de acuerdo con la política específica de la organización en materia de control de acceso y otras políticas específicas relacionadas, así como con los requisitos de la empresa, teniendo en cuenta la legislación aplicable.

Propósito

Limitar la exposición de datos sensibles, incluida la información de identificación personal, y cumplir los requisitos legales, estatutarios, reglamentarios y contractuales.

Orientación

Cuando la protección de datos sensibles (por ejemplo, la IPI) sea una preocupación, la organización debe considerar la posibilidad de ocultar dichos datos utilizando técnicas como el enmascaramiento de datos, la seudonimización o la anonimización.

Las técnicas de seudonimización o anonimización pueden ocultar la IIP, disimular la verdadera identidad de los titulares de la IIP u otra información sensible, y desconectar el vínculo entre la IIP y la identidad del titular de la IIP o el vínculo entre otra información sensible.

Cuando se utilicen técnicas de seudonimización o anonimización, deberá verificarse que los datos han sido adecuadamente seudonimizados o anonimizados. La anonimización de datos debe considerar todos los elementos de la información sensible para ser eficaz. Por ejemplo, si no se consideran adecuadamente, se puede identificar a una persona, aunque se anonimicen los datos que pueden identificarla directamente, por la presencia de otros datos que permiten identificarla indirectamente.

Otras técnicas de enmascaramiento de datos son

a) el cifrado (que requiere que los usuarios autorizados dispongan de una clave);
b) anulación o supresión de caracteres (impidiendo que los usuarios no autorizados vean los mensajes completos);
c) variación de números y fechas
d) sustitución (cambiar un valor por otro para ocultar datos sensibles);
e) sustitución de valores por su hash.

Al aplicar las técnicas de enmascaramiento de datos debe tenerse en cuenta lo siguiente:

a) no conceder a todos los usuarios acceso a todos los datos; por tanto, diseñar consultas y máscaras para mostrar al usuario sólo los datos mínimos necesarios;

b) hay casos en los que algunos datos no deben ser visibles para el usuario para algunos registros de un conjunto de datos; en este caso, diseñar y aplicar un mecanismo de ofuscación de datos (por ejemplo, si un paciente no quiere que el personal del hospital pueda ver todos sus registros, incluso en caso de emergencia, entonces al personal del hospital se le presentan datos parcialmente ofuscados y sólo puede acceder a los datos el personal con funciones específicas si contienen información útil para un tratamiento adecuado);
c) cuando los datos están ofuscados, dando al responsable de la IIP la posibilidad de exigir que los usuarios no puedan ver si los datos están ofuscados (ofuscación de la ofuscación; esto se utiliza en centros sanitarios, por ejemplo, si el paciente no quiere que el personal vea que se ha ofuscado información sensible como embarazos o resultados de análisis de sangre);
d) cualquier requisito legal o reglamentario (por ejemplo, exigir el enmascaramiento de la información de las tarjetas de pago durante su procesamiento o almacenamiento).

Al utilizar el enmascaramiento, la seudonimización o la anonimización de datos, debe tenerse en cuenta lo siguiente

a) nivel de intensidad del enmascaramiento, seudonimización o anonimización de datos en función del uso de los datos tratados;
b) controles de acceso a los datos tratados
c) acuerdos o restricciones sobre el uso de los datos tratados
d) la prohibición de cotejar los datos tratados con otra información con el fin de identificar al interesado principal;
e) llevar un registro del suministro y la recepción de los datos tratados.

Otra información

La anonimización altera de forma irreversible la IPI de tal manera que el titular de la IPI ya no puede ser identificado directa o indirectamente.

La seudonimización sustituye la información identificativa por un alias. El conocimiento del algoritmo (a veces denominado "información adicional") utilizado para llevar a cabo la seudonimización permite al menos algún tipo de identificación del titular de la IPI. Por lo tanto, dicha "información adicional" debe mantenerse separada y protegida.

Aunque la seudonimización es, por tanto, más débil que la anonimización, los conjuntos de datos seudonimizados pueden ser más útiles en la investigación estadística.

El enmascaramiento de datos es un conjunto de técnicas para ocultar, sustituir u ofuscar elementos de datos sensibles. El enmascaramiento de datos puede ser estático (cuando los elementos de datos se enmascaran en la base de datos original), dinámico (utilizando automatización y reglas para asegurar los datos en tiempo real) o sobre la marcha (con datos enmascarados en la memoria de una aplicación).

Pueden utilizarse funciones hash para anonimizar la IPI. Para evitar ataques de enumeración, siempre deben combinarse con una función de sal.

La IPI en identificadores de recursos y sus atributos [por ejemplo, nombres de archivos, localizadores uniformes de recursos (URL)] debe evitarse o anonimizarse adecuadamente.

A8.12 Prevención de fuga de datos.

Tabla 4646. Generalidades A8.12 Prevención de fuga de datos.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Detección	-Confidencialidad	-Proteger -Detectar	-Protección de la información	-Protección -Defensa

Controlar

Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

Propósito

Detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Orientación

La organización debe tener en cuenta lo siguiente para reducir el riesgo de fuga de datos:

a) identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos);
b) controlar los canales de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y dispositivos de almacenamiento portátiles);
c) actuar para evitar la fuga de información (por ejemplo, poner en cuarentena los correos electrónicos que contengan información sensible).

Las herramientas de prevención de fuga de datos deben utilizarse para:

a) identificar y controlar la información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos no estructurados en el sistema de un usuario);
b) detectar la divulgación de información sensible (por ejemplo, cuando la información se carga en servicios en la nube de terceros no fiables o se envía por correo electrónico);
c) bloquear acciones del usuario o transmisiones de red que expongan información sensible (por ejemplo, impedir la copia de entradas de bases de datos en una hoja de cálculo).

La organización debe determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos en servicios, dispositivos y medios de almacenamiento fuera de la organización. Si ese es el caso, la organización debe implementar tecnología como herramientas de prevención de fuga de datos o la configuración de herramientas existentes que permitan a los usuarios ver y manipular datos mantenidos de forma remota pero que impidan copiar y pegar fuera del control de la organización.

Si es necesario exportar datos, el propietario de los datos debe poder aprobar la exportación y responsabilizar a los usuarios de sus acciones.

La realización de capturas de pantalla o fotografías de la pantalla debe abordarse mediante condiciones de uso, formación y auditoría.

Cuando se realicen copias de seguridad de los datos, hay que asegurarse de que la información sensible está protegida con medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen la copia de seguridad.

La prevención de la fuga de datos también debe tenerse en cuenta para protegerse contra las acciones de inteligencia de un adversario que obtenga información confidencial o secreta (geopolítica, humana, financiera, comercial, científica o de cualquier otro tipo) que pueda ser de interés para el espionaje o pueda ser crítica para la comunidad. Las acciones de prevención de fuga de datos deben estar orientadas a confundir las decisiones del adversario, por ejemplo, sustituyendo información auténtica por información falsa, ya sea como acción independiente o como respuesta a las acciones de inteligencia del adversario. Ejemplos de este tipo de acciones son la ingeniería social inversa o el uso de honeypots para atraer a los atacantes.

Otra información

Las herramientas de prevención de fuga de datos están diseñadas para identificar datos, supervisar su uso y movimiento y tomar medidas para evitar que se filtren (por ejemplo, alertando a los usuarios de su comportamiento arriesgado y bloqueando la transferencia de datos a dispositivos de almacenamiento portátiles).

La prevención de la fuga de datos implica intrínsecamente el control de las comunicaciones y actividades en línea del personal y, por extensión, de los mensajes de terceros, lo que plantea problemas legales que deben tenerse en cuenta antes de desplegar herramientas de prevención de la fuga de datos. Existe una variedad de legislación relativa a la privacidad, la protección de datos, el empleo, la interceptación de datos y las telecomunicaciones que es aplicable a la supervisión y el tratamiento de datos en el contexto de la prevención de fuga de datos.

La prevención de fuga de datos puede apoyarse en controles de seguridad estándar, como políticas específicas sobre control de acceso y gestión segura de documentos.

A8.13 Copia de seguridad de la información.

Tabla 4747. Generalidades A8.13 Copia de seguridad de la información.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Correctivo	-Integridad -Disponibilidad	-Recuperar	-Continuidad	-Protección

Controlar

Las copias de seguridad de la información, el software y los sistemas deben mantenerse y comprobarse periódicamente de acuerdo con la política específica acordada sobre copias de seguridad.

Propósito

Permitir la recuperación en caso de pérdida de datos o sistemas.

Orientación

Debe establecerse una política temática específica sobre copias de seguridad para abordar los requisitos de retención de datos y seguridad de la información de la organización.

Deben proporcionarse instalaciones de copia de seguridad adecuadas para garantizar que toda la información y el software esenciales puedan recuperarse tras un incidente, fallo o pérdida de los medios de almacenamiento.

Deben desarrollarse e implementarse planes sobre cómo la organización realizará copias de seguridad de la información, el software y los sistemas, para abordar la política específica sobre copias de seguridad.

Al diseñar un plan de copias de seguridad, deben tenerse en cuenta los siguientes aspectos

a) elaborar registros precisos y completos de las copias de seguridad y de los procedimientos de restauración documentados;
b) reflejar los requisitos empresariales de la organización (por ejemplo, el objetivo del punto de recuperación), los requisitos de seguridad de la información implicada y el carácter crítico de la información para el funcionamiento continuado de la organización en el alcance (por ejemplo, copia de seguridad completa o diferencial) y la frecuencia de las copias de seguridad;
c) almacenar las copias de seguridad en una ubicación remota segura y protegida, a una distancia suficiente para escapar de cualquier daño derivado de un desastre en el sitio principal;
d) proporcionar a la información de las copias de seguridad un nivel adecuado de protección física y medioambiental coherente con las normas aplicadas en el emplazamiento principal;

e) probar periódicamente los soportes de las copias de seguridad para garantizar que pueden utilizarse en caso de emergencia cuando sea necesario. Probar la capacidad de restaurar los datos de las copias de seguridad en un sistema de prueba, no sobrescribiendo el soporte de almacenamiento original en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas irreparables de datos;
f) Proteger las copias de seguridad mediante cifrado en función de los riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad sea importante);
g) asegurarse de que se detecta una pérdida involuntaria de datos antes de realizar la copia de seguridad.

Los procedimientos operativos deben supervisar la ejecución de las copias de seguridad y abordar los fallos de las copias de seguridad programadas para garantizar la integridad de las copias de seguridad de acuerdo con la política específica sobre copias de seguridad.

Las medidas de copia de seguridad de los distintos sistemas y servicios deben probarse periódicamente para garantizar que cumplen los objetivos de los planes de respuesta a incidentes y de continuidad de las actividades. Esto debe combinarse con una prueba de los procedimientos de restauración y cotejarse con el tiempo de restauración requerido por el plan de continuidad del negocio. En el caso de sistemas y servicios críticos, las medidas de copia de seguridad deben cubrir toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de desastre.

Cuando la organización utilice un servicio en la nube, deben realizarse copias de seguridad de la información, las aplicaciones y los sistemas de la organización en el entorno del servicio en la nube. La organización debe determinar si se cumplen los requisitos para la realización de copias de seguridad cuando se utiliza el servicio de copia de seguridad de la información proporcionado como parte del servicio en nube, y de qué manera.

Debe determinarse el período de conservación de la información empresarial esencial, teniendo en cuenta cualquier requisito de conservación de copias de archivo. La organización debe considerar la eliminación de la información en los medios de almacenamiento utilizados para las copias de seguridad una vez que expire el período de conservación de la información y debe tener en cuenta la legislación y la normativa.

A8.15 Registro

Tabla 4848. Generalidades A8.15 Registro.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Detección	-Confidencialidad -Integridad -Disponibilidad	-Detección	-Gestión de eventos de seguridad de la información	-Protección -Defensa

Control

Deben elaborarse, almacenarse, protegerse y analizarse registros de actividades, excepciones, fallos y otros eventos relevantes.

Propósito

Registrar eventos, generar pruebas, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que puedan conducir a un incidente de seguridad de la información y apoyar las investigaciones.

Orientación

Generalidades

La organización debe determinar el propósito para el que se crean los registros, qué datos se recopilan y registran, y cualquier requisito específico para proteger y manejar los datos de registro. Esto debe documentarse en una política específica sobre registros.

Los registros de eventos deben incluir para cada evento, según corresponda

a) ID de usuario;
b) actividades del sistema
c) fechas, horas y detalles de los eventos relevantes (por ejemplo, inicio y cierre de sesión);
d) identidad del dispositivo, identificador del sistema y ubicación;
e) direcciones y protocolos de red.

Los siguientes eventos deben ser considerados para el registro:

a) intentos exitosos y rechazados de acceso al sistema;
b) intentos exitosos y rechazados de acceso a datos y otros recursos;
c) cambios en la configuración del sistema
d) uso de privilegios
e) uso de programas de utilidad y aplicaciones
f) archivos a los que se ha accedido y tipo de acceso, incluida la eliminación de archivos de datos importantes;
g) alarmas emitidas por el sistema de control de acceso;
h) activación y desactivación de sistemas de seguridad, como sistemas antivirus y sistemas de detección de intrusos;

i) creación, modificación o supresión de identidades
j) transacciones ejecutadas por los usuarios en las aplicaciones. En algunos casos, las aplicaciones son un servicio o producto prestado o gestionado por un tercero.

Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas, ya que esto permite la correlación de registros entre sistemas para el análisis, alerta e investigación de un incidente.

Protección de los registros

Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deben tener permiso para borrar o desactivar los registros de sus propias actividades. Pueden manipular potencialmente los registros de las instalaciones de tratamiento de la información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios privilegiados.

Los controles deben tener como objetivo la protección contra cambios no autorizados en la información de los registros y problemas operativos con la instalación de registro, incluyendo:

a) alteraciones de los tipos de mensajes que se registran;
b) edición o eliminación de archivos de registro
c) que no se registren eventos o que se sobrescriban eventos registrados anteriormente si se excede el medio de almacenamiento que contiene un archivo de registro.

Para la protección de los registros, se debe considerar el uso de las siguientes técnicas: hashing criptográfico, registro en un archivo de sólo apéndice y sólo lectura, registro en un archivo de transparencia pública.

Puede ser necesario archivar algunos registros de auditoría debido a requisitos de conservación de datos o requisitos de recopilación y conservación de pruebas.

Cuando la organización necesite enviar registros de sistemas o aplicaciones a un proveedor para ayudar a depurar o solucionar errores, los registros deben de Identificarse en la medida de lo posible utilizando técnicas de enmascaramiento de datos para información como nombres de usuario, direcciones de protocolo de Internet (IP), nombres de host o nombre de la organización, antes de enviarlos al proveedor.

Los registros de eventos pueden contener datos sensibles e información personal identificable. Deben adoptarse medidas adecuadas de protección de la privacidad.

Análisis de registros

El análisis de registros debe abarcar el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividades inusuales o comportamientos anómalos, que pueden representar indicadores de compromiso.

El análisis de eventos debe realizarse teniendo en cuenta

a) las competencias necesarias de los expertos que realizan el análisis;
b) la determinación del procedimiento de análisis de registros
c) los atributos necesarios de cada evento relacionado con la seguridad

d) las excepciones identificadas mediante el uso de reglas predeterminadas [por ejemplo, información de seguridad y gestión de eventos (SIEM) o reglas de cortafuegos, y sistemas de detección de intrusiones (IDS) o firmas de malware];
e) patrones de comportamiento conocidos y tráfico de red estándar comparados con actividades y comportamientos anómalos [análisis del comportamiento de usuarios y entidades (UEBA)
f) resultados de análisis de tendencias o patrones (por ejemplo, como resultado del uso de análisis de datos, técnicas de big data y herramientas de análisis especializadas)
g) información disponible sobre amenazas.

El análisis de registros debe apoyarse en actividades de supervisión específicas que ayuden a identificar y analizar comportamientos anómalos, lo que incluye

a) revisar los intentos exitosos y fallidos de acceder a recursos protegidos [por ejemplo, servidores del sistema de nombres de dominio (DNS), portales web y archivos compartidos];
b) comprobación de los registros DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados a servidores de mando y control de botnets;
c) examen de los informes de uso de los proveedores de servicios (por ejemplo, facturas o informes de servicio) para detectar actividades inusuales en los sistemas y redes (por ejemplo, revisando patrones de actividad)
d) incluyendo registros de eventos de supervisión física, como entradas y salidas, para garantizar una detección y un análisis de incidentes más precisos;
e) correlacionar los registros para permitir un análisis eficaz y de gran precisión.

Los incidentes de seguridad de la información presuntos y reales deben ser identificados (por ejemplo, infección por malware o sondeo de cortafuegos) y ser objeto de una investigación posterior (por ejemplo, como parte de un proceso de gestión de incidentes de seguridad de la información).

Otra información

Los registros del sistema suelen contener un gran volumen de información, mucha de la cual es ajena a la supervisión de la seguridad de la información. Para ayudar a identificar eventos significativos para la supervisión de la seguridad de la información, se puede considerar el uso de programas de utilidad adecuados o herramientas de auditoría para realizar la interrogación de archivos.

El registro de eventos sienta las bases para sistemas de supervisión automatizados capaces de generar informes consolidados y alertas sobre la seguridad del sistema.

Se puede utilizar una herramienta SIEM o un servicio equivalente para almacenar, correlacionar, normalizar y analizar la información de registro, y para generar alertas. Los SIEM suelen requerir una configuración cuidadosa para optimizar sus beneficios. Las configuraciones a tener en cuenta incluyen la identificación y selección de fuentes de registro apropiadas, el ajuste y prueba de reglas y el desarrollo de casos de uso.

Los archivos de transparencia pública para el registro de logs se utilizan, por ejemplo, en los sistemas de transparencia de certificados. Estos archivos pueden proporcionar un mecanismo de detección adicional útil para protegerse de la manipulación de registros.

En los entornos en nube, las responsabilidades de gestión de registros pueden ser compartidas entre el cliente del servicio en nube y el proveedor del servicio en nube.

A8.16 Actividades de supervisión

Tabla 4949. Generalidades A8.16 Actividades de supervisión.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Detección -Corrección	-Confidencialidad -Integridad -Disponibilidad	-Detección -Respuesta	-Gestión de eventos de seguridad de la información	-Defensa

Control

Se deben supervisar las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y tomar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

Propósito

Detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

Orientación

El alcance y el nivel de la supervisión deben determinarse de acuerdo con los requisitos empresariales y de seguridad de la información y teniendo en cuenta las leyes y reglamentos pertinentes. Los registros de supervisión deben conservarse durante períodos definidos.

Debe considerarse la inclusión de los siguientes aspectos en el sistema de supervisión:

a) tráfico saliente y entrante de la red, del sistema y de las aplicaciones;
b) acceso a sistemas, servidores, equipos de red, sistema de supervisión, aplicaciones críticas, etc.;
c) archivos de configuración de red y de sistemas críticos o de nivel de administrador;
d) registros de herramientas de seguridad [por ejemplo, antivirus, IDS, sistema de prevención de intrusiones (IPS), filtros web, cortafuegos, prevención de fuga de datos];
e) registros de eventos relativos a la actividad del sistema y de la red;
f) comprobación de que el código que se está ejecutando está autorizado a ejecutarse en el sistema y que no ha sido manipulado (por ejemplo, mediante la recompilación para añadir código adicional no deseado);
g) el uso de los recursos (por ejemplo, CPU, discos duros, memoria, ancho de banda) y su rendimiento.

La organización debe establecer una línea de base del comportamiento normal y controlar las anomalías con respecto a esta línea de base. Al establecer una línea de base, debe tenerse en cuenta lo siguiente:

a) la revisión de la utilización de los sistemas en periodos normales y punta;
b) la hora habitual de acceso, el lugar de acceso y la frecuencia de acceso de cada usuario o grupo de usuarios.

El sistema de supervisión debe configurarse en función de la línea de base establecida para identificar comportamientos anómalos, como:

a) terminación no planificada de procesos o aplicaciones;
b) actividad típicamente asociada a malware o tráfico procedente de direcciones IP o dominios de red maliciosos conocidos (por ejemplo, los asociados a servidores de mando y control de botnets);
c) características de ataque conocidas (por ejemplo, denegación de servicio y desbordamientos de búfer)
d) comportamiento inusual del sistema (por ejemplo, registro de pulsaciones de teclas, inyección de procesos y desviaciones en el uso de protocolos estándar);
e) cuellos de botella y sobrecargas (por ejemplo, colas en la red, niveles de latencia y fluctuación de la red);
f) acceso no autorizado (real o intentado) a sistemas o información
g) exploración no autorizada de aplicaciones, sistemas y redes empresariales
h) intentos exitosos e infructuosos de acceder a recursos protegidos (por ejemplo, servidores DNS, portales web y sistemas de archivos);
i) comportamiento inusual de usuarios y sistemas en relación con el comportamiento esperado.

Debe utilizarse una herramienta de supervisión continua. La supervisión debe realizarse en tiempo real o a intervalos periódicos, en función de las necesidades y capacidades de la organización. Las herramientas de supervisión deben tener la capacidad de manejar grandes cantidades de datos, adaptarse a un panorama de amenazas en constante cambio y permitir la notificación en tiempo real. Las herramientas también deben ser capaces de reconocer firmas y datos específicos o patrones de comportamiento de redes o aplicaciones.

El software de supervisión automatizada debe estar configurado para generar alertas (por ejemplo, a través de consolas de gestión, mensajes de correo electrónico o sistemas de mensajería instantánea) basadas en umbrales predefinidos. El sistema de alerta debe ser ajustado y entrenado en la línea de base de la organización para minimizar los falsos positivos.

El personal debe estar dedicado a responder a las alertas y debe recibir la formación adecuada para interpretar con precisión los posibles incidentes. Debe haber sistemas y procesos redundantes para recibir y responder a las notificaciones de alerta.

Los sucesos anómalos deben comunicarse a las partes pertinentes para mejorar las siguientes actividades: auditoría, evaluación de la seguridad, exploración de vulnerabilidades y supervisión. Deben establecerse procedimientos para responder oportunamente a los indicadores positivos del sistema de vigilancia, a fin de minimizar el efecto de los eventos adversos sobre la seguridad de la información. También deben establecerse procedimientos para identificar y tratar los falsos positivos, incluido el ajuste del software de supervisión para reducir el número de falsos positivos en el futuro.

Otras informaciones

La supervisión de la seguridad puede mejorarse:

a) aprovechando los sistemas de inteligencia sobre amenazas
b) aprovechando las capacidades de aprendizaje automático e inteligencia artificial;
c) el uso de listas de bloqueo o listas permitidas;
d) la realización de una serie de evaluaciones técnicas de seguridad (por ejemplo, evaluaciones de vulnerabilidad, pruebas de penetración, simulaciones de ciberataques y ejercicios de ciberrespuesta), y la utilización de los resultados de estas evaluaciones para ayudar a determinar las líneas de base o el comportamiento aceptable;
e) utilización de sistemas de supervisión del rendimiento para ayudar a establecer y detectar comportamientos anómalos
f) aprovechar los registros en combinación con los sistemas de supervisión.

A menudo, las actividades de supervisión se llevan a cabo mediante programas informáticos especializados, como los sistemas de detección de intrusos. Éstos pueden configurarse para una línea de base de actividades normales, aceptables y esperadas del sistema y la red.

La supervisión de las comunicaciones anómalas ayuda a identificar las botnets (es decir, el conjunto de dispositivos bajo el control malicioso del propietario de la botnet, que suele utilizarse para montar ataques distribuidos de denegación de servicio contra otros ordenadores de otras organizaciones). Si el ordenador está siendo controlado por un dispositivo externo, existe una comunicación entre el dispositivo infectado y el controlador. Por lo tanto, la organización debe emplear tecnologías para vigilar las comunicaciones anómalas y tomar las medidas necesarias.

A8.18 Uso de programas de utilidad privilegiados

Tabla 5050. Generalidades A8.18 Uso de programas de utilidad privilegiados.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad del sistema y de la red -Configuración segura -Seguridad de las aplicaciones	-Protección

Control

El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.

Propósito

Garantizar que el uso de programas de utilidades no perjudique los controles de sistemas y aplicaciones para la seguridad de la información.

Orientación

Deben tenerse en cuenta las siguientes directrices para el uso de programas de utilidades que puedan anular los controles del sistema y de las aplicaciones:

a) limitación del uso de programas de utilidades al número mínimo práctico de usuarios autorizados y de confianza;
b) utilización de procedimientos de identificación, autenticación y autorización para los programas de utilidades, incluida la identificación única de la persona que utiliza el programa de utilidades;
c) definición y documentación de los niveles de autorización para los programas de utilidades
d) autorización para el uso ad hoc de programas de utilidades;
e) no poner los programas de utilidades a disposición de usuarios que tengan acceso a aplicaciones en sistemas en los que se requiera la segregación de funciones;
f) eliminar o desactivar todos los programas de utilidades innecesarios;
g) como mínimo, segregación lógica de los programas de utilidades del software de aplicación. Cuando resulte práctico, segregar las comunicaciones de red para dichos programas del tráfico de aplicaciones;
h) limitación de la disponibilidad de los programas de utilidades (por ejemplo, mientras dure un cambio autorizado)
i) registro de todo uso de programas de utilidades.

Otra información

La mayoría de los sistemas de información disponen de uno o varios programas de utilidad capaces de anular los controles del sistema y de las aplicaciones, por ejemplo, diagnósticos, parches, antivirus, desfragmentadores de disco, depuradores, herramientas de copia de seguridad y de red.

A8.19 Instalación de software en sistemas operativos

Tabla 5151. Generalidades A8.19 Instalación de software en sistemas operativos.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Configuración segura -Seguridad de las aplicaciones	-Protección

Controlar

Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

Propósito

Garantizar la integridad de los sistemas operativos y evitar la explotación de vulnerabilidades técnicas.

Orientación

Deben tenerse en cuenta las siguientes directrices para gestionar de forma segura los cambios y la instalación de software en los sistemas operativos:

a) realizar las actualizaciones del software operativo únicamente por administradores formados previa autorización de la dirección;
b) garantizar que en los sistemas operativos sólo se instala código ejecutable aprobado y no código de desarrollo ni compiladores;
c) instalar y actualizar el software sólo después de haber realizado pruebas exhaustivas y satisfactorias
d) actualizar todas las bibliotecas de fuentes de programas correspondientes
e) utilizar un sistema de control de la configuración para mantener el control de todo el software operativo, así como de la documentación del sistema;
f) definir una estrategia de reversión antes de aplicar los cambios
g) mantener un registro de auditoría de todas las actualizaciones del software operativo;
h) archivar las versiones antiguas del software, junto con toda la información y los parámetros necesarios, los procedimientos, los detalles de configuración y el software de apoyo como medida de contingencia, y mientras se requiera que el software lea o procese los datos archivados.

Cualquier decisión de actualizar a una nueva versión debe tener en cuenta los requisitos empresariales para el cambio y la seguridad de la versión (por ejemplo, la introducción de nuevas funciones de seguridad de la información o el número y la gravedad de las vulnerabilidades de seguridad de la información que afectan a la versión actual). Los parches de software deben aplicarse cuando puedan ayudar a eliminar o reducir las vulnerabilidades de seguridad de la información.

Los programas informáticos pueden basarse en programas y paquetes suministrados externamente (por ejemplo, programas informáticos que utilizan módulos alojados en sitios externos), que deben supervisarse y controlarse para evitar cambios no autorizados, ya que pueden introducir vulnerabilidades en la seguridad de la información.

Los programas informáticos suministrados por proveedores y utilizados en sistemas operativos deben mantenerse a un nivel soportado por el proveedor. Con el tiempo, los proveedores de software dejarán de dar soporte a versiones antiguas de software. La organización debe considerar los riesgos de confiar en software no soportado. El software de código abierto utilizado en los sistemas operativos debe mantenerse hasta la última versión adecuada del software. Con el tiempo, el código fuente abierto puede dejar de mantenerse, pero sigue estando disponible en un repositorio de software de código abierto. La organización también debe tener en cuenta los riesgos de confiar en software de código abierto no mantenido cuando se utiliza en sistemas operativos.

Cuando los proveedores participen en la instalación o actualización de programas informáticos, el acceso físico o lógico sólo debe concederse cuando sea necesario y con la debida autorización. Se deben supervisar las actividades del proveedor.

La organización debe definir y aplicar normas estrictas sobre qué tipos de software pueden instalar los usuarios.

Debe aplicarse el principio del menor privilegio a la instalación de software en los sistemas operativos. La organización debe identificar qué tipos de instalaciones de software están permitidas (por ejemplo, actualizaciones y parches de seguridad para el software existente) y qué tipos de instalaciones están prohibidas (por ejemplo, software que es sólo para uso personal y software cuyo pedigrí con respecto a ser potencialmente malicioso es desconocido o sospechoso). Estos privilegios deben concederse en función de las funciones de los usuarios afectados.

A8.20 Seguridad de redes

Tabla 5252. Generalidades A8.20 Seguridad de redes.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Detección	- Confidencialidad -Integridad -Disponibilidad	-Proteger -Detectar	-Seguridad de sistemas y redes	-Protección

Controlar

Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información de los sistemas y aplicaciones.

Propósito

Proteger la información en las redes y sus instalaciones de procesamiento de información de apoyo contra el peligro a través de la red.

Orientación

Deben implantarse controles para garantizar la seguridad de la información en las redes y proteger los servicios conectados de accesos no autorizados. En particular, deben tenerse en cuenta los siguientes aspectos

a) el tipo y nivel de clasificación de la información que puede soportar la red;
b) el establecimiento de responsabilidades y procedimientos para la gestión de los equipos y dispositivos de la red
c) mantener actualizada la documentación, incluidos los diagramas de red y los archivos de configuración de los dispositivos (por ejemplo, enrutadores, conmutadores);
d) separar, cuando proceda, la responsabilidad operativa de las redes de las operaciones de los sistemas TIC;
e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas y para proteger los sistemas y aplicaciones conectados. También pueden ser necesarios controles adicionales para mantener la disponibilidad de los servicios de red y de los ordenadores conectados a la red
f) registrar y supervisar adecuadamente para permitir el registro y la detección de acciones que puedan afectar a la seguridad de la información o sean relevantes para ella
g) coordinar estrechamente las actividades de gestión de la red tanto para optimizar el servicio a la organización como para garantizar que los controles se aplican de forma coherente en toda la infraestructura de tratamiento de la información;
h) autenticar los sistemas en la red;
i) restringir y filtrar la conexión de sistemas a la red (por ejemplo, mediante cortafuegos);
j) detección, restricción y autenticación de la conexión de equipos y dispositivos a la red;

k) endurecimiento de los dispositivos de red
l) segregación de los canales de administración de la red del resto del tráfico de la red;
m) aislar temporalmente las subredes críticas (por ejemplo, con puentes levadizos) si la red sufre un ataque;
n) desactivar los protocolos de red vulnerables.

La organización debe garantizar que se aplican los controles de seguridad adecuados al uso de redes virtualizadas. Las redes virtualizadas también abarcan las redes definidas por software (SDN, SD-WAN). Las redes virtualizadas pueden ser deseables desde el punto de vista de la seguridad, ya que pueden permitir la separación lógica de la comunicación que tiene lugar a través de redes físicas, en particular para sistemas y aplicaciones que se implementan utilizando computación distribuida.

A8.21 Seguridad en los servicios de red

Tabla 5353. Generalidades A8.21 Seguridad en los servicios de red.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad de sistemas y redes	-Protección

Controlar

Deben identificarse, aplicarse y controlarse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

Propósito

Garantizar la seguridad en el uso de los servicios de red.

Orientación

Las medidas de seguridad necesarias para determinados servicios, como los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio, deben identificarse e implementarse (por proveedores de servicios de red internos o externos). La organización debe asegurarse de que los proveedores de servicios de red aplican estas medidas.

Debe determinarse y supervisarse periódicamente la capacidad del proveedor de servicios de red para gestionar de forma segura los servicios acordados. La organización y el proveedor deben acordar el derecho de auditoría. La organización también debe tener en cuenta los certificados de terceros proporcionados por los proveedores de servicios para demostrar que mantienen las medidas de seguridad adecuadas.

Deben formularse y aplicarse normas sobre el uso de redes y servicios de red que abarquen

a) las redes y servicios de red a los que se permite acceder;
b) los requisitos de autenticación para acceder a los distintos servicios de red
c) los procedimientos de autorización para determinar quién puede acceder a qué redes y servicios de red
a) servicios en red;
d) los controles y procedimientos tecnológicos y de gestión de la red para proteger el acceso a las conexiones de red y a los servicios de red
e) los medios utilizados para acceder a las redes y a los servicios de red [por ejemplo, el uso de una red privada virtual (VPN) o de una red inalámbrica]
f) hora, ubicación y otros atributos del usuario en el momento del acceso
g) supervisión del uso de los servicios de red.

Deben tenerse en cuenta las siguientes características de seguridad de los servicios de red

a) tecnología aplicada para la seguridad de los servicios de red, como autenticación, cifrado y controles de conexión a la red;
b) parámetros técnicos necesarios para la conexión segura con los servicios de red de conformidad con las normas de seguridad y conexión a la red
c) el almacenamiento en caché (por ejemplo, en una red de distribución de contenidos) y sus parámetros, que permiten a los usuarios elegir el uso del almacenamiento en caché de acuerdo con los requisitos de rendimiento, disponibilidad y confidencialidad
d) procedimientos para que el uso del servicio de red restrinja el acceso a los servicios o aplicaciones de red, cuando sea necesario.

Información adicional

Los servicios de red incluyen el suministro de conexiones, servicios de red privada y soluciones de seguridad de red gestionadas, como cortafuegos y sistemas de detección de intrusos. Estos servicios pueden ir desde un simple ancho de banda no gestionado hasta complejas ofertas de valor añadido.

A8.24 Uso de criptografía.

Tabla 5454. Generalidades A8.24 Uso de criptografía.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Configuración segura	-Protección

Controlar

Deben definirse y aplicarse normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

Propósito

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información de acuerdo con los requisitos empresariales y de seguridad de la información, y teniendo en cuenta

consideración los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.

Orientación

Generalidades

Al utilizar criptografía, se debe tener en cuenta lo siguiente:

a) la política específica sobre criptografía definida por la organización, incluidos los principios generales para la protección de la información. Una política temática específica sobre el uso de la criptografía es necesaria para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y para evitar un uso inapropiado o incorrecto;
b) la identificación del nivel de protección requerido y la clasificación de la información y, en consecuencia, el establecimiento del tipo, la fuerza y la calidad de los algoritmos criptográficos necesarios
c) el uso de la criptografía para la protección de la información contenida en dispositivos móviles de usuario final o medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento
d) el enfoque de la gestión de claves, incluidos los métodos para tratar la generación y protección de claves criptográficas y la recuperación de la información cifrada en caso de pérdida, compromiso o deterioro de las claves
e) funciones y responsabilidades para:
    1. la aplicación de las normas para el uso eficaz de la criptografía
    2. la gestión de claves, incluida la generación de claves

f) las normas que deben adoptarse, así como los algoritmos criptográficos, la fuerza de cifrado, las soluciones criptográficas y las prácticas de uso que se aprueben o exijan para su utilización en la organización
g) el impacto del uso de información cifrada en los controles que se basan en la inspección de contenidos (por ejemplo, detección de malware o filtrado de contenidos).

Al aplicar las normas de la organización para el uso eficaz de la criptografía, deben tenerse en cuenta las normativas y restricciones nacionales que pueden aplicarse al uso de técnicas criptográficas en distintas partes del mundo, así como las cuestiones relativas al flujo transfronterizo de información cifrada.

El contenido de los acuerdos de nivel de servicio o de los contratos con proveedores externos de servicios criptográficos (por ejemplo, con una autoridad de certificación) debe cubrir cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta para la prestación de los servicios.

Gestión de claves

Una gestión de claves adecuada requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Un sistema de gestión de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;
b) emisión y obtención de certificados de clave pública
c) la distribución de claves a las entidades previstas, incluido el modo de activar las claves cuando se reciben
d) el almacenamiento de claves, incluido el modo en que los usuarios autorizados obtienen acceso a las claves
e) el cambio o actualización de claves, incluidas las normas sobre cuándo cambiar las claves y cómo hacerlo
f) tratamiento de las claves comprometidas
g) la revocación de claves, incluida la forma de retirarlas o desactivarlas [por ejemplo, cuando las claves se han visto comprometidas o cuando un usuario abandona la organización (en cuyo caso las claves también deben archivarse)];
h) Recuperación de claves perdidas o dañadas;
i) realizar copias de seguridad o archivar claves;
j) destrucción de claves;
k) registro y auditoría de las actividades relacionadas con la gestión de claves;
l) fijación de fechas de activación y desactivación de las claves, de modo que éstas sólo puedan utilizarse durante el periodo de tiempo que establezcan las normas de la organización en materia de gestión de claves;
m) gestionar las solicitudes legales de acceso a claves criptográficas (por ejemplo, se puede exigir que la información cifrada esté disponible de forma no cifrada como prueba en un juicio).

Todas las claves criptográficas deben estar protegidas contra modificaciones y pérdidas. Además, las claves secretas y privadas deben protegerse contra el uso no autorizado y la

divulgación. Los equipos utilizados para generar, almacenar y archivar claves deben estar protegidos físicamente.

Además de la integridad, en muchos casos de uso también debe tenerse en cuenta la autenticidad de las claves públicas.

Otra información

La autenticidad de las claves públicas suele abordarse mediante procesos de gestión de claves públicas que utilizan autoridades de certificación y certificados de clave pública, pero también es posible abordarla mediante tecnologías como la aplicación de procesos manuales para claves de pequeño número.

La criptografía puede utilizarse para alcanzar diferentes objetivos de seguridad de la información, por ejemplo:

a) confidencialidad: utilización del cifrado de la información para proteger la información sensible o crítica, almacenada o transmitida;
b) integridad o autenticidad: utilización de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información sensible o crítica almacenada o transmitida. Utilización de algoritmos para comprobar la integridad de los ficheros;
c) no repudio: utilización de técnicas criptográficas para proporcionar pruebas de la ocurrencia o no ocurrencia de un evento o acción;
d) autenticación: utilización de técnicas criptográficas para autenticar a los usuarios y otras entidades del sistema que soliciten acceso o realicen transacciones con usuarios, entidades y recursos del sistema.

A8.25 Ciclo de vida de desarrollo seguro.

Tabla 5555. Generalidades A8.25 Ciclo de vida de desarrollo seguro.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad de las aplicaciones -Seguridad de sistemas y redes	-Protección

Controlar

Deben establecerse y aplicarse normas para el desarrollo seguro de software y sistemas.

Propósito

Garantizar que la seguridad de la información se diseña e implementa dentro del ciclo de vida de desarrollo seguro de software y sistemas.

Orientación

El desarrollo seguro es un requisito para construir un servicio, una arquitectura, un software y un sistema seguros. Para lograrlo, deben tenerse en cuenta los siguientes aspectos

a) separación de los entornos de desarrollo, prueba y producción;
b) orientación sobre la seguridad en el ciclo de vida del desarrollo de software:
    1) seguridad en la metodología de desarrollo de software
    2) directrices de codificación segura para cada lenguaje de programación utilizado
c) requisitos de seguridad en la fase de especificación y diseño
d) puntos de control de la seguridad en los proyectos
e) pruebas de seguridad y del sistema, como pruebas de regresión, escaneado de código y pruebas de penetración;
f) repositorios seguros para el código fuente y la configuración;
g) seguridad en el control de versiones;
h) conocimientos y formación necesarios en materia de seguridad de las aplicaciones
i) capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades;
j) requisitos de licencia y alternativas para garantizar soluciones rentables y evitar futuros problemas de licencia.

Si se subcontrata el desarrollo, la organización debe obtener garantías de que el proveedor cumple las normas de la organización para un desarrollo seguro.

Otra información

El desarrollo también puede tener lugar dentro de aplicaciones, como aplicaciones ofimáticas, scripts, navegadores y bases de datos.

A8.29 Pruebas de seguridad en desarrollo y aceptación.

Tabla 5656. Generalidades A8.29 Pruebas de seguridad en desarrollo y aceptación.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Identidad	-Seguridad en Aplicaciones. -Garantía en seguridad de la información -Seguridad en sistemas y redes.	-Protección.

Control

Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.

Propósito

Para validar si se cumplen los requisitos de seguridad de la información cuando se implementan aplicaciones o código en el entorno de producción.

Orientación

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deben probarse y verificarse minuciosamente durante los procesos de desarrollo. Las pruebas de seguridad deben ser una parte integral de las pruebas de los sistemas o componentes, Las pruebas de seguridad deben realizarse frente a un conjunto de requisitos, que se pueden expresar como funcional o no funcional. Las pruebas de seguridad deben incluir pruebas de:

a) funciones de seguridad [p. autenticación de usuario (ver 8.5), restricción de acceso (ver 8.3) y uso de criptografía;

b) codificación segura;

c) configuraciones seguras (ver 8.9, 8.20 y 8.22) incluyendo la de sistemas operativos, firewalls y

otros componentes de seguridad.

Los planes de prueba deben determinarse utilizando un conjunto de criterios. El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo.

El plan de pruebas debe incluir:

a) cronograma detallado de actividades y pruebas;

b) insumos y productos esperados bajo una variedad de condiciones;

c) criterios para evaluar los resultados;

d) decisión de acciones adicionales según sea necesario.

La organización puede aprovechar herramientas automatizadas, como herramientas de análisis de código o escáneres de vulnerabilidades, y debe verificar la corrección de los defectos relacionados con la seguridad.

Para los desarrollos internos, estas pruebas deben ser realizadas inicialmente por el equipo de desarrollo.

Luego se deben realizar pruebas de aceptación independientes para garantizar que el sistema funcione como se espera y solo como se esperaba.

Se debe considerar lo siguiente:

a) realizar actividades de revisión de código como un elemento relevante para la prueba de fallas de seguridad, incluidas las imprevistas entradas y condiciones;

b) realizar un escaneo de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) realizar pruebas de penetración para identificar código y diseño inseguros.

Para los componentes de compra y desarrollo subcontratados, se debe seguir un proceso de adquisición.

Los contratos con el proveedor deben abordar los requisitos de seguridad, identificando productos y los servicios deben evaluarse según estos criterios antes de la adquisición.

Las pruebas deben realizarse en un entorno de prueba que coincida con el entorno de producción de destino, lo más cerca posible para garantizar que el sistema no introduzca vulnerabilidades en el sistema de la organización y que las pruebas sean confiables.

Otra información

Se pueden establecer múltiples entornos de prueba, que se pueden usar para diferentes tipos de pruebas, por ejemplo, pruebas funcionales y de rendimiento. Estos diferentes entornos pueden ser virtuales, con personas las configuraciones para simular una variedad de entornos operativos.

También se debe considerar la prueba y el monitoreo de entornos, herramientas y tecnologías de prueba para asegurar pruebas efectivas. Las mismas consideraciones se aplican a monitoreo de los sistemas de monitorización implementada en entornos de desarrollo, prueba y producción. Se necesita juicio, guiado por la sensibilidad de los sistemas y datos, para determinar cuántas capas de meta-testing son útiles.

A8.3 Restricción de acceso a la información.

Tabla 5757. Generalidades A8.3 Restricción de acceso a la información.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Identidad y administración de accesos.	-Protección.

Control

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con las

estableció una política temática específica sobre el control de acceso.

Propósito

Para garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros

activos asociados.

Orientación

El acceso a la información y otros activos asociados debe estar restringido de acuerdo con las

políticas establecidas sobre temas específicos. Debe tenerse en cuenta lo siguiente para facilitar el acceso requisitos de restricción:

a) no permitir el acceso a información sensible por parte de usuarios con identidades desconocidas o de forma anónima. Público o el acceso anónimo solo debe otorgarse a ubicaciones de almacenamiento que no contengan datos confidenciales de información;

b) proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios;

c) controlar a qué datos puede acceder un usuario en particular;

d) controlar qué identidades o grupo de identidades tienen qué acceso, como lectura, escritura, eliminación y ejecutar;

e) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, aplicaciones, datos o sistemas.

Además, las técnicas y procesos de gestión de acceso dinámico para proteger la información confidencial que tiene un alto valor para la organización deben ser considerado cuando la organización:

a) necesita un control granular sobre quién puede acceder a dicha información durante qué período y de qué manera;

b) quiere compartir dicha información con personas ajenas a la organización y mantener el control sobre quién puede acceder a él;

c) quiere gestionar dinámicamente, en tiempo real, el uso y distribución de dicha información;

d) quiere proteger dicha información contra cambios no autorizados, copia y distribución

(incluida la impresión);

e) quiere monitorear el uso de la información;

f) quiere registrar cualquier cambio en dicha información que tenga lugar en caso de que se lleve a cabo una investigación futura requerido.

Las técnicas de gestión de acceso dinámico deben proteger la información a lo largo de su ciclo de vida (es decir, creación, procesamiento, almacenamiento, transmisión y disposición), incluyendo:

a) establecer reglas sobre la gestión del acceso dinámico en función de casos de uso específicos considerando:

1) otorgar permisos de acceso en función de la identidad, el dispositivo, la ubicación o la aplicación;

2) aprovechar el esquema de clasificación para determinar qué información debe ser

protegido con técnicas de gestión de acceso dinámico;

b) establecer procesos operativos, de seguimiento y de presentación de informes y apoyo técnico infraestructura.

Los sistemas de gestión de acceso dinámico deben proteger la información mediante:

a) exigir autenticación, credenciales apropiadas o un certificado para acceder a la información;

b) restringir el acceso, por ejemplo, a un período de tiempo específico (por ejemplo, después de una fecha determinada o hasta un determinado

fecha);

c) usar cifrado para proteger la información;

d) definir los permisos de impresión de la información;

e) registrar quién accede a la información y cómo se utiliza la información;

f) generar alertas si se detectan intentos de mal uso de la información.

Otra información

Las técnicas de gestión de acceso dinámico y otras tecnologías de protección de información dinámica pueden apoyar la protección de la información incluso cuando los datos se comparten más allá de la organización de origen, donde los controles de acceso tradicionales no se pueden hacer cumplir. Se puede aplicar a documentos, correos electrónicos u otros archivos que contienen información para limitar quién puede acceder al contenido y de qué manera. Puede ser en un granular y adaptarse a lo largo del ciclo de vida de la información.

Las técnicas de gestión de acceso dinámico no reemplazan la gestión de acceso clásica [p. usando el acceso listas de control (ACL)], pero puede agregar más factores para condicionalidad, evaluación en tiempo real, datos justo a tiempo reducción y otras mejoras que pueden ser útiles para la información más sensible. ofrece una forma de controlar el acceso fuera del entorno de la organización. La respuesta a incidentes puede ser apoyada por técnicas de gestión de acceso dinámico, ya que los permisos se pueden modificar o revocar en cualquier momento.

A8.32 Gestión del cambio.

Tabla 5858. Generalidades A8.32 Gestión del cambio.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad en Aplicaciones. -Seguridad en sistemas y redes.	-Protección.

Control

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a cambios procedimientos de gestión.

Propósito

Preservar la seguridad de la información al ejecutar cambios.

Orientación

La introducción de nuevos sistemas y cambios importantes en los sistemas existentes debe seguir reglas acordadas y un proceso formal de documentación, especificación, prueba, control de calidad e implementación administrada.

Deben existir responsabilidades y procedimientos de gestión para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de información en instalaciones de procesamiento de información y sistemas de información, para todo el ciclo de vida de desarrollo del sistema desde las primeras etapas de diseño hasta todo el mantenimiento posterior esfuerzos.

Siempre que sea factible, los procedimientos de control de cambios para la infraestructura y el software de TIC deben ser integrado.

Los procedimientos de control de cambios deben incluir:

a) planificar y evaluar el impacto potencial de los cambios considerando todas las dependencias;

b) autorización de cambios;

c) comunicar los cambios a las partes interesadas relevantes;

d) pruebas y aceptación de pruebas para los cambios;

e) implementación de cambios, incluidos los planes de implementación;

f) consideraciones de emergencia y contingencia, incluidos los procedimientos de respaldo;

g) mantener registros de cambios que incluyan todo lo anterior;

h) asegurar que la documentación operativa y los procedimientos del usuario se cambien según sea necesario permanecer apropiado;

i) garantizar que se cambien los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación según sea necesario para seguir siendo apropiado.

Otra información.

El control inadecuado de los cambios en las instalaciones de procesamiento de información y los sistemas de información es una causa común de fallas del sistema o de seguridad. Los cambios en el entorno de producción, especialmente cuando la transferencia de software del entorno de desarrollo al entorno operativo puede tener un impacto en la integridad y disponibilidad de aplicaciones.

Cambiar el software puede afectar el entorno de producción y viceversa.

La buena práctica incluye la prueba de los componentes de las TIC en un entorno segregado tanto del

entornos de producción y desarrollo (ver 8.31). Esto proporciona un medio de tener control sobre

nuevo software y que permite una protección adicional de la información operativa que se utiliza para las pruebas propósitos Esto debería incluir parches, paquetes de servicio y otras actualizaciones.

El entorno de producción incluye sistemas operativos, bases de datos y plataformas de middleware. El control debe aplicarse para cambios de aplicaciones e infraestructuras.

A8.5 Autenticación Segura.

Tabla 5959. Generalidades A8.5 Autenticación Segura.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Identidad y administración de accesos.	-Protección.

Control

Deben implementarse tecnologías y procedimientos de autenticación seguros basados en información restricciones de acceso y la política específica del tema sobre el control de acceso.

Propósito

Para garantizar que un usuario o una entidad esté autenticado de forma segura, cuando el acceso a sistemas, aplicaciones y se otorgan los servicios.

Orientación

Se debe elegir una técnica de autenticación adecuada para corroborar la identidad reclamada de un usuario, software, mensajes y otras entidades.

La fuerza de autenticación debe ser apropiada para la clasificación de la información a ser accedido. Cuando se requiera una fuerte autenticación y verificación de identidad, los métodos de autenticación alternativas a las contraseñas, como certificados digitales, tarjetas inteligentes, tokens o medios biométricos, deben ser usado.

La información de autenticación debe ir acompañada de factores de autenticación adicionales para acceder sistemas de información crítico, también conocida como autenticación multifactor. Usando una combinación de múltiples factores de autenticación, como lo que sabes, lo que tienes y lo que eres, reduce las posibilidades de accesos no autorizados. La autenticación multifactor se puede combinar con otras técnicas para requerir factores adicionales bajo circunstancias específicas, basadas en reglas predefinidas y patrones, como el acceso desde una ubicación inusual, desde un dispositivo inusual o en un momento inusual.

La información de autenticación biométrica debe invalidarse si alguna vez se ve comprometida. Biométrico la autenticación puede no estar disponible dependiendo de las condiciones de uso, por ejemplo, humedad o envejecimiento. A prepararse para estos problemas, la autenticación biométrica debe ir acompañada de al menos una alternativa técnica de autenticación.

El procedimiento para iniciar sesión en un sistema o aplicación debe estar diseñado para minimizar el riesgo de acceso no autorizado. Los procedimientos y tecnologías de inicio de sesión deben implementarse teniendo en cuenta la siguiente:

a) no mostrar información confidencial del sistema o de la aplicación hasta que se haya completado el proceso de inicio de sesión completado con éxito para evitar proporcionar a un usuario no autorizado cualquier información innecesaria asistencia;

b) mostrar un aviso general advirtiendo que el sistema o la aplicación o el servicio solo debe ser accedido por usuarios autorizados;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayudarían a un usuario no autorizado, por ejemplo: si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecto;

d) validar la información de inicio de sesión solo al completar todos los datos de entrada;

e) protección contra intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas [p. usando completamente, Prueba de Turing pública automatizada para diferenciar computadoras y humanos, que requiere contraseña restablecer después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores;

f) registrar intentos fallidos y exitosos;

g) generar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de inicio de sesión, por ejemplo: enviar una alerta al usuario y a los administradores del sistema de la organización cuando se ha alcanzado el número de intentos de contraseña incorrectos);

h) mostrar o enviar la siguiente información en un canal separado al completarse con éxito iniciar sesión:

1) fecha y hora del inicio de sesión exitoso anterior;

2) detalles de cualquier intento fallido de inicio de sesión desde el último inicio de sesión exitoso;

i) no mostrar una contraseña en texto claro cuando se ingresa; en algunos casos, puede ser necesario desactivar esta funcionalidad para facilitar el inicio de sesión del usuario, por ejemplo: por razones de accesibilidad o para evitar el bloqueo de usuarios por errores repetidos);

j) no transmitir contraseñas en texto claro a través de una red para evitar ser capturado por una red programa "sniffer";

k) finalizar sesiones inactivas después de un período definido de inactividad, especialmente en ubicaciones de alto riesgo tales como áreas públicas o externas fuera de la gestión de seguridad de la organización o en el usuario dispositivos de punto final;

l) restringir los tiempos de duración de la conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

A8.6 Gestión de la capacidad.

Tabla 6060. Generalidades A8.6 Gestión de la capacidad.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Detectar	-Integridad -Disponibilidad	-Identificar -Proteger -Detectar	-Continuidad	-Gobernanza y Ecosistema -Protección.

Control

El uso de los recursos debe monitorearse y ajustarse de acuerdo con la capacidad actual y esperada de requisitos.

Propósito

Asegurar la capacidad requerida de las instalaciones de procesamiento de información, recursos humanos, oficinas y otras instalaciones.

Orientación

Requisitos de capacidad para instalaciones de procesamiento de información, recursos humanos, oficinas y otros deben identificarse las instalaciones, teniendo en cuenta la criticidad comercial de los sistemas en cuestión y procesos.

Se debe aplicar el ajuste y monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas.

La organización debe realizar pruebas de estrés de los sistemas y servicios para confirmar que el sistema suficiente de la capacidad está disponible para cumplir con los requisitos de rendimiento máximo.

Deben establecerse controles de detección para indicar los problemas a su debido tiempo.

Las proyecciones de los futuros requisitos de capacidad deben tener en cuenta los nuevos negocios y sistemas.

requisitos y tendencias actuales y proyectadas en el procesamiento de la información de la capacidad de la organización.

Se debe prestar especial atención a cualquier recurso con largos plazos de entrega o altos costos.

Por lo tanto, los gerentes, propietarios de servicios o productos deben monitorear la utilización de los recursos clave del sistema.

Los administradores deben usar la información de capacidad para identificar y evitar posibles limitaciones de recursos y dependencia del personal clave que puede representar una amenaza para la seguridad del sistema o los servicios y el plan acción apropiada.

Se puede lograr proporcionar capacidad suficiente aumentando la capacidad o reduciendo la demanda.

Se debe considerar lo siguiente para aumentar la capacidad:

a) contratación de nuevo personal;

b) obtención de nuevas instalaciones o espacio;

c) adquirir sistemas de procesamiento, memoria y almacenamiento más potentes;

d) hacer uso de la computación en la nube, que tiene características inherentes que abordan directamente cuestiones de capacidad. La computación en la nube tiene elasticidad y escalabilidad que permiten una rápida expansión bajo demanda y reducción de los recursos disponibles para aplicaciones y servicios particulares.

Se debe considerar lo siguiente para reducir la demanda de los recursos de la organización:

a) eliminación de datos obsoletos (espacio en disco);

b) eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio en los estantes);

c) desmantelamiento de aplicaciones, sistemas, bases de datos o entornos;

d) optimizar procesos por lotes y cronogramas;

e) optimizar el código de la aplicación o las consultas de la base de datos;

f) denegar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos.

Se debe considerar un plan de gestión de capacidad documentado para los sistemas de misión crítica.

Otra información

Para obtener más detalles sobre la elasticidad y la escalabilidad de la computación en la nube.

A8.7 Protección contra malware.

Tabla 6161. Generalidades A8.7 Protección contra malware.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo -Detectar -Correctivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger -Detectar	-Protección en la Configuración. - Seguridad en sistemas y redes.	-Protección -Defender

Control

La protección contra el malware debe implementarse y respaldarse mediante la conciencia adecuada del usuario.

Propósito

Para garantizar que la información y otros activos asociados estén protegidos contra malware.

Orientación

La protección contra malware debe basarse en software de detección y reparación de malware, información conciencia de seguridad, acceso apropiado al sistema y controles de gestión de cambios. uso de malware.

El software de detección y reparación por sí solo no suele ser adecuado. La siguiente guía debe ser consideró:

a) implementar reglas y controles que prevengan o detecten el uso de software no autorizado, por ejemplo: lista de aplicaciones permitidas (es decir, usar una lista que proporciona aplicaciones permitidas);

b) implementar controles que prevengan o detecten el uso de sitios web maliciosos conocidos o sospechosos (por ejemplo, listas de bloqueo);

c) reducir las vulnerabilidades que pueden ser explotadas por malware [p. a través de la vulnerabilidad técnica gestión;

d) llevar a cabo una validación automatizada regular del software y el contenido de datos de los sistemas, especialmente para sistemas que soportan procesos comerciales críticos; investigando la presencia de cualquier no aprobado archivos o modificaciones no autorizadas;

e) establecer medidas de protección contra los riesgos asociados con la obtención de archivos y software ya sea desde o a través de redes externas o en cualquier otro medio;

f) instalar y actualizar regularmente software de detección y reparación de malware para escanear computadoras y medios de almacenamiento electrónicos. Realización de escaneos regulares que incluyen:

1) escanear cualquier dato recibido a través de redes o a través de cualquier forma de medio de almacenamiento electrónico, para malware antes de su uso;

2) escanear archivos adjuntos y descargas de correo electrónico y mensajería instantánea en busca de malware antes de su uso.

Llevar a cabo este escaneo en diferentes lugares (por ejemplo, en servidores de correo electrónico, computadoras de escritorio) y cuando ingresar a la red de la organización;

3) escanear páginas web en busca de malware cuando se accede a ellas;

g) determinar la ubicación y configuración de las herramientas de detección y reparación de malware en función del riesgo resultados de la evaluación y considerando:

1) principios de defensa en profundidad donde serían más efectivos. Por ejemplo, esto puede conducir a detección de malware en una puerta de enlace de red (en varios protocolos de aplicación como correo electrónico, archivo transferencia y web), así como servidores y dispositivos de punto final de usuario;

2) las técnicas evasivas de los atacantes (p. ej., el uso de archivos cifrados) para entregar malware o el uso de protocolos de encriptación para transmitir malware;

h) tener cuidado de proteger contra la introducción de malware durante el mantenimiento y emergencia procedimientos, que pueden eludir los controles normales contra el malware;

i) implementar un proceso para autorizar la inhabilitación temporal o permanente de algunas o todas las medidas contra malware, incluidas las autoridades de aprobación de excepciones, justificación documentada y revisión fecha. Esto puede ser necesario cuando la protección contra el malware provoca una interrupción del funcionamiento normal de operaciones;

j) preparar planes apropiados de continuidad comercial para recuperarse de ataques de malware, incluidos todas las copias de seguridad de datos y software necesarias (incluidas las copias de seguridad en línea y fuera de línea) y la recuperación medidas.

k) aislar ambientes donde puedan ocurrir consecuencias catastróficas;

l) definir procedimientos y responsabilidades para tratar la protección contra malware en los sistemas, incluida la capacitación en su uso, informes y recuperación de ataques de malware;

m) proporcionar conciencia o capacitación a todos los usuarios sobre cómo identificar y mitigar potencialmente la recepción, envío o instalación de correos electrónicos, archivos o programas infectados con malware, la información recogida en n) y o) pueden utilizarse para garantizar que la concienciación y la formación se mantengan actualizadas;

n) implementar procedimientos para recopilar periódicamente información sobre nuevo malware, como suscribirse a listas de correo o revisando sitios web relevantes;
o) verificar que la información relacionada con el malware, como los boletines de advertencia, proviene de personal calificado y fuentes confiables, por ejemplo, sitios de Internet confiables o proveedores de software de detección de malware y es preciso e informativo.

Otra información

No siempre es posible instalar software que protege contra malware en algunos sistemas, por ejemplo, algunos sistemas de control industrial. Algunas formas de malware infectan los sistemas operativos y las computadoras firmware tal que los controles de malware comunes no pueden limpiar el sistema y una nueva imagen completa del software del sistema operativo y, a veces, el firmware de la computadora es necesario para volver a un entorno de estado seguro.

A8.9 Gestión de la configuración.

Tabla 6262. Generalidades A8.9 Gestión de la configuración.

Tipo Control	Propiedades de seguridad de información	Conceptos Ciberseguridad	Capacidades Operacionales	Dominios de seguridad
-Preventivo	-Confidencialidad -Integridad -Disponibilidad	-Proteger	-Seguridad en la Configuración.	-Protección

Control.
Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

Propósito
Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la seguridad requerida ajustes, y la configuración no se altera por cambios no autorizados o incorrectos.

Orientación
General
La organización debe definir e implementar procesos y herramientas para hacer cumplir las configuraciones definidas.
(incluidas las configuraciones de seguridad) para hardware, software, servicios (por ejemplo, servicios en la nube) y redes, para los sistemas recién instalados, así como para los sistemas operativos durante su vida útil.
Deben existir roles, responsabilidades y procedimientos para asegurar un control satisfactorio de todos cambios de configuración.

Plantillas estándar.
Las plantillas estándar para la configuración segura de hardware, software, servicios y redes deberían definirse:

a) utilizando orientación disponible públicamente (por ejemplo: plantillas predefinidas de proveedores y de fuentes independientes). organizaciones de seguridad);
b) considerar el nivel de protección necesario para determinar un nivel suficiente de seguridad;

c) respaldar la política de seguridad de la información de la organización, las políticas específicas del tema, los estándares y otros requisitos de seguridad;

d) considerar la viabilidad y aplicabilidad de las configuraciones de seguridad en el contexto de la organización.

Las plantillas deben revisarse periódicamente y actualizarse cuando se necesiten nuevas amenazas o vulnerabilidades. a tratar, o cuando se introducen nuevas versiones de software o hardware.

Se debe considerar lo siguiente para establecer plantillas estándar para la configuración segura de hardware, software, servicios y redes:

a) minimizar el número de identidades con derechos de acceso privilegiados o de nivel de administrador;

b) deshabilitar identidades innecesarias, no utilizadas o inseguras;

c) deshabilitar o restringir funciones y servicios innecesarios;

d) restringir el acceso a poderosos programas de utilidades y configuraciones de parámetros del host;

e) sincronización de relojes;

f) cambiar la información de autenticación predeterminada del proveedor, como las contraseñas predeterminadas, inmediatamente después instalación y revisión de otros parámetros importantes relacionados con la seguridad predeterminados;

g) invocar las instalaciones de tiempo de espera que cierran automáticamente la sesión de los dispositivos informáticos después de un tiempo predeterminado período de inactividad;

h) verificar que se han cumplido los requisitos de la licencia.

Administrar configuraciones.

Las configuraciones establecidas de hardware, software, servicios y redes deben registrarse y un registro debe mantenerse de todos los cambios de configuración. Estos registros deben almacenarse de forma segura. Esto puede lograrse de varias maneras, como bases de datos de configuración o plantillas de configuración.

Los cambios en las configuraciones deben seguir el proceso de gestión de cambios.

Los registros de configuración pueden contener según corresponda:

a) información actualizada del propietario o punto de contacto del activo;

b) fecha del último cambio de configuración;

c) versión de la plantilla de configuración;

d) relación con configuraciones de otros activos.

Monitoreo de configuraciones

Las configuraciones deben monitorearse con un conjunto integral de herramientas de administración del sistema (por ejemplo: utilidades de mantenimiento, soporte remoto, herramientas de gestión empresarial, software de copia de seguridad y restauración) y debe revisarse periódicamente para verificar los ajustes de configuración, evaluar la seguridad de las contraseñas y evaluar las actividades realizadas. Las configuraciones reales se pueden comparar con el objetivo definido plantillas. Cualquier desviación debe abordarse, ya sea mediante la aplicación automática del objetivo definido configuración o por análisis manual de la desviación seguido de acciones correctivas.

Otra información.

La documentación de los sistemas a menudo registra detalles sobre la configuración del hardware y software.

El endurecimiento del sistema es una parte típica de la gestión de la configuración.

La gestión de la configuración se puede integrar con los procesos de gestión de activos y las herramientas asociadas.

La automatización suele ser más efectiva para administrar la configuración de seguridad (por ejemplo, usar la infraestructura como código).

Las plantillas de configuración y los destinos pueden ser información confidencial y deben protegerse de acceso no autorizado en consecuencia.

Capítulo IV: Entrega de Resultados

Informe de resultados

En conformidad con el Plan, se ha realizado la revisión de los controles referentes a A5, A6, A7 y A8 en la cooperativa de la que se detalla a continuación el estándar a evaluar en la auditoria, la sección de controles, los hallazgos, los comentarios en base a la ISO 27001 (ISO/IEC 27001 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, 2013).

La evaluación y revisión que debe ser elaborada a todos los recursos informáticos que se encuentran en las áreas responsables del procesamiento de información que se encuentren funcionando y con lleven al buen funcionamiento y al mejor desempeño de la Cooperativa, para brindar una mejor atención a sus asociados. Partiendo de la autorización por parte del Consejo de Administración “Diseño de un Sistema de Gestión de Seguridad de la Información para la Cooperativa Financiera SIHUACOOP DE R.L., dedicada a brindar servicios financieros de Ahorro y Crédito en la ciudad de Santa Ana.”, mediante el cual se realizó la evaluación de los procedimientos que sigue la empresa.

En la auditoría realizada a SIHUACOOP denotamos la falta de conocimiento y conciencia acerca de las mejores prácticas de controles internos y auditoría de los sistemas de información por parte de las autoridades de la cooperativa y del personal que está relacionado con las tecnologías de información y comunicaciones.

Algunas condiciones que se han presentado en la evaluación son:

- Las autoridades de la cooperativa SIHUACOOP y las unidades de la empresa, en conjunto con los proveedores externos y los usuarios, han realizado un análisis de los servicios de tecnología de la empresa, basados en sus características básicas, procedimientos que soportan y su nivel de importancia para la Cooperativa, lo cual imposibilita que se definan controles a los activos informáticos que normalicen la disponibilidad y el funcionamiento adecuado de los activos informáticos brindados.

- El procedimiento de la gestión de los activos, se tiene un inventario de todos los activos, con un propietario de activo, el cual hace un buen uso del activo que tiene a cargo, asimismo se tiene una clasificación de los activos y etiquetado que se podría mejorar, Tienen políticas para el buen manejo de los medios.

- La Cooperativa SIHUACOOP DE R.L., tiene un buen manejo de control de accesos a las áreas restringidas, buen control y políticas para la gestión de los usuarios, debería incluir las medidas de seguridad adoptadas por la empresa en un plan de seguridad, de manera que en caso de la existencia de algún incidente o modificación errónea se pueda regresar a la configuración adecuada de los sistemas.

- LA SIHUACOOP DE R.L., tiene un plan de continuidad de la empresa y dan seguimiento, en el que se incluye análisis de las operaciones y servicios críticos proporcionados, los recursos de hardware y software que permiten la ejecución de estas operaciones, riesgos naturales y tecnológicos que pueden afectar a los mencionados recursos, el personal clave encargado de la ejecución y recuperación de las operaciones debe ser un especialista que este dedicado a este tipo de actividades, tienen un centro alterno de operación como replica ubicado en la nube. Dentro de este plan se debe considerar la obtención y almacenamiento de respaldos de la información que permitan la recuperación inmediata de los datos.

La siguiente escala de evaluación detalla el nivel que se puede obtener en la evaluación de un control específico, esto en base a la norma ISO.

Tabla 6363. ISO 27001:2022 Escala de evaluación.

0 – Inexistente	1 – Inicial / Ad hoc	2 – Repetible pero intuitivo	3 – Definido	4 – Gestionado y medible	5 – Optimizado
No se reconoce la necesidad de un proceso.	Hay pruebas de que la empresa ha reconocido que los problemas existen y deben abordarse.	El proceso ahora se implementa, pero es posible que no esté documentado, y generalmente depende del conocimiento y la motivación de las personas.	El proceso ahora se implementa utilizando un proceso definido que es capaz de lograr los resultados deseados.	El proceso ahora opera dentro de umbrales definidos para lograr sus resultados.	El proceso se mejora continuamente para cumplir con los objetivos comerciales actuales y proyectados relevantes (basados en autoevaluaciones y análisis de brechas y causa raíz).
El proceso no se implementa.	El enfoque de los requisitos de riesgo y control es ad hoc y desorganizado, sin comunicación ni monitoreo (y tiende a aplicarse de forma individual o caso por caso).	La eficacia no se evalúa adecuadamente.	La efectividad operativa se evalúa periódicamente.	Una evaluación formal documentada del proceso ocurre con frecuencia.	Las oportunidades de mejora derivadas de las nuevas tecnologías y conceptos de procesos se identifican, miden y actúan.
Existe un alto riesgo de deficiencias e incidentes.	No se identifican deficiencias.	Existen muchas debilidades y, si no se abordan adecuadamente, el impacto puede ser grave.	La gerencia es capaz de lidiar de manera predecible con la mayoría de los problemas, pero persisten algunas debilidades y los impactos aún podrían ser graves.	Se supervisa el cumplimiento y se toman las medidas apropiadas.	Se definen los objetivos de mejora de procesos que respaldan los objetivos comerciales relevantes.
En este nivel hay poca o ninguna evidencia de algún logro sistemático del propósito del proceso.	Los empleados no son conscientes de sus responsabilidades.	Las acciones de la gerencia para resolver problemas no son priorizadas ni consistentes.	Los procedimientos son obligatorios; Sin embargo, puede ser poco probable que se detecten todas las desviaciones.	Se establecen y miden objetivos cuantitativos para el rendimiento del proceso en apoyo de los objetivos comerciales relevantes.	Se ha asignado plena responsabilidad para el monitoreo de procesos, la gestión de riesgos y la aplicación del cumplimiento.
	El proceso implementado logra su propósito y resultados definidos.	Los empleados pueden no ser conscientes de sus responsabilidades.	El proceso y los procedimientos que lo acompañan se han comunicado a través de la capacitación.	Es probable que la administración detecte la mayoría de los problemas, pero no todos los problemas se identifican de forma rutinaria.	Los empleados participan proactivamente en las mejoras de control.

				Existe un seguimiento constante para abordar las deficiencias identificadas.	
				Se han implementado automatización y herramientas.	

Detalle de evaluación de los controles detallados para el diseño de un sistema de gestión de seguridad de la información para la Cooperativa SIHUACOOP DE R.L.

Tabla 6464. ISO 27001:2022 Detalle evaluación de controles.

Estándar		Sección	Hallazgos	Nivel MMC
A.5 Controles Organizacionales				**2**
A5.1	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas del tema serán definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	* Existe una política definida para seguridad, pero no hay muestras que se actualice de forma periódica. * No se ha definido la aplicabilidad de la política, se debe establecer quienes deben cumplirla * No se ha divulgado a las demás áreas, la existencia de una política	3
A5.2	Funciones y responsabilidades de seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	La Cooperativa muestra conciencia en sus debilidades en relación a roles y funciones de seguridad de la información. Pero no se han realizado aun proyectos para subsanar estas deficiencias debido a presupuesto y falta de planeación.	1
A5.3	Separación de funciones	**Control** Las funciones conflictivas y los ámbitos de responsabilidad conflictivos se separarán.	* Existe una definición de roles, aunque no tan detallada como debería ser; si hay una conciencia y documentación de que se deben segregar las funciones. * Aun no están definidos roles específicos para seguridad de la información * Hay escaso personal para todas las funciones que lleva actualmente el departamento * Presupuesto para contratación de personal nuevo es limitado, se debe hacer conciencia a la Gerencia General de esta necesidad para asegurar la continuidad del negocio	3

A5.4	Responsabilidades de gestión	**Control** La gerencia requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos del tema de la organización.	* No se ha socializado la política de seguridad a toda la organización, por lo cual los empleados no son conscientes de sus responsabilidades en temas de seguridad de la información * Ya que no se ha socializado, no podemos determinar que hay gestión alguna de la correcta implementación y control de la política.	1
A5.5	Contacto con las autoridades	**Control** La organización debe establecer y mantener contacto con las autoridades pertinentes.	* Existe un oficial de cumplimiento en la organización * Se realizan auditorías internas y externas para confirmar cumplimiento y rendir cuentas a junta de vigilancia y gerencias * Se deben presentar informes de forma periódica a autoridades que regulen las cooperativas: INSAFOCOOP, BCR, Super intendencia del Sistema Financiero, Ministerio de Hacienda y Consejo de Administración Interno.	4
A5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	No existe evidencia que la Cooperativa sea parte de ningún grupo de esta índole, adicionalmente no hay obligaciones legales que requieran cumplimiento de ser parte de este tipo de foros o grupos. Se recomienda tomar en cuenta el ser miembro de algún grupo a nivel nacional o internacional para poder estar actualizados en noticias de seguridad que pudieran o mejorar los procesos o ayudar a detectar ataques de forma temprana y anticipada.	0
A5.7	Inteligencia de amenazas	**Control** La información relativa a las amenazas a la seguridad de la información se recopilará y analizará para producir información sobre amenazas.	No hay evidencia que sustente este punto	0
A5.8	Seguridad de la información en la gestión de proyectos	**Control**	No hay evidencia que sustente este punto	0

		La seguridad de la información se integrará en la gestión del proyecto.		
A5.9	Inventario de información y otros activos asociados	**Control** Se elaborará y mantendrá un inventario de la información y otros activos asociados, incluidos los propietarios.	Si hay un inventario de activos, pero no se pudo observar dentro los servicios y estos también son considerados activos importantes para la Cooperativa, por lo que se recomienda también incluirlos dentro del inventario.	3
A5.10	Uso aceptable de la información y otros activos asociados	**Control** Se identificarán, documentarán y aplicarán normas para el uso aceptable y los procedimientos para el manejo de la información y otros activos asociados.	El uso aceptable de los activos está definido dentro de la política de seguridad	3
A5.11	Devolución de activos	**Control** El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su poder al cambiar o terminar su empleo, contrato o acuerdo.	* Dentro del proceso de desvinculación de empleados, se toma en cuenta la desactivación de credenciales, pero no la entrega o devolución de equipo informático asignado. * Se debe incluir dentro de la política las normativas a seguir para devolución de equipo en caso de despido o renuncia voluntaria del personal.	1
A5.12	Clasificación de la información	**Control** La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la disponibilidad de integridad y los requisitos pertinentes de las partes interesadas.	* Política contempla la clasificación de la información y establece como responsable de esta tarea al Encargado de Seguridad de Información. * Aun no existe el rol de Encargado de Seguridad de Información, por lo cual este proceso esta únicamente definido, pero no es gestionable o medible.	3
A5.13	Etiquetado de la información	**Control** Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.	* Se ha establecido dentro de la política la clasificación, pero no hay evidencias de un proceso establecido aún. * En la política se menciona que los lineamientos se establecerán por el Encargado de Seguridad de la información, aun no hay un recurso dentro de la compañía que cumpla esta función.	1

A5.14	Transferencia de información	**Control** Las reglas, procedimientos o acuerdos de transferencia de información deben estar en su lugar para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	* Esta establecido dentro de la política que para compartir información se deberá hacer de forma cifrada y comprimida para dificultar su acceso no autorizado, además de mostrar el nivel de clasificación (reservada o restringida) * Unidades que generan o gestionan información clasificada deberán guardar su información en ubicaciones de red especifico donde se han definido accesos en base a las necesidades de los puestos que acceden a ella * Se hacen copias de respaldo en nube y dispositivos externos	3
A5.15	Control de acceso	**Control** Se establecerán y aplicarán normas para controlar el acceso físico y lógico a la información y otros activos asociados sobre la base de los requisitos empresariales y de seguridad de la información.	* Existen controles de acceso físico a data center * Se comparte el espacio para guardar copias de seguridad físicas con otras unidades, lo cual puede llevar a una perdida no controlada de la información o a ser expuesta a personal externo a IT * Se ha definido dentro de la política controles de acceso en relación a: Redes, Administración de Usuarios, Responsabilidades de los Usuarios, Altos privilegios y Utilitarios de la Administración y Acceso a Sistemas y aplicativos.	3
A5.16	Gestión de la identidad	**Control** Se gestionará todo el ciclo de vida de las identidades.	* Política establece que se deben gestionar los accesos a los diferentes sistemas y dominios de control * Política también contempla que se deben revocar accesos en los casos donde se estime conveniente como: despidos y renuncias	4
A5.17	Información de autenticación	**Control** La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al	* Política establece las normas para asignación y gestión de autenticación, pero no hay evidencias que exista un proceso de asesoramiento.	3

		personal sobre el tratamiento adecuado de la información de autenticación.		
A5.18	Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados deben ser proporcionados, revisados, modificados y eliminados de acuerdo con la política específica de la organización y las normas de control de acceso. y eliminados de acuerdo con la política específica de la organización y las normas de control de acceso.	* política establece las normas para asignación y gestión de autenticación a dominio organización y sistemas empresariales	4
A5.19	Seguridad de la información en las relaciones con los proveedores	**Control** Deben definirse y aplicarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios del proveedor.	* Política establece que proveedores de servicios y personal externo deben adoptar los lineamientos establecidos en la política * Política establece que deberán existir penalizaciones en caso se incumplan los lineamientos establecidos en la política * Se ha establecido dentro de la política lineamientos para el otorgamiento de acceso a redes, uso de periféricos e información crítica de la cooperativa	4
A5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	**Control** Los requisitos pertinentes de seguridad de la información se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.	* Dentro de la relación contractual se establecen de forma general los acuerdos de servicios y seguridad * Requisitos se establecen en la política de forma general pero no hay evidencia que se categorice en base al tipo de proveedor o los tipos de relaciones que establecen con los mismos	2
A5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y la comunicación (TIC)	**Control** Deben definirse y aplicarse procesos y procedimientos implantados para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.	* Dentro de la relación contractual se establecen de forma general los acuerdos de servicios y seguridad * Existe conocimiento de la importancia de la seguridad en la relación de los proveedores, pero no hay controles que establezcan seguridad en la cadena de	1

			suministro de la prestación de estos servicios.	
A5.22	Monitoreo, revisión y gestión del cambio de los servicios de los proveedores	**Control** La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información del proveedor y la prestación de servicios.	* No existen aún, monitoreo en las prácticas de seguridad de los proveedores	1
A5.23	Seguridad de la información para el uso de servicios en la nube	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización.	* Organización utiliza la nube para cumplir con las políticas de redundancia, pero no hay un proceso de adquisición establecido, así como la gestión de recursos y seguridad.	1
A5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	**Control** La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, funciones y responsabilidades de gestión de incidentes de seguridad de la información.	* Existe la iniciativa para la detección de riesgos por la Unidad de Riesgos de la organización, pero no hay proceso de planificación y preparación de la gestión de incidentes de Seguridad Informática	1
A5.25	Evaluación y decisión sobre eventos de seguridad en la información	**Control** La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.	* Existe la iniciativa para la detección de riesgos por la Unidad de Riesgos de la organización, pero no hay proceso de planificación y preparación de la gestión de incidentes de Seguridad Informática	1
A5.26	Respuesta a incidentes de seguridad de la información	**Control** Los incidentes de seguridad de la información se responderán de acuerdo con los procedimientos documentados.	* No hay un plan establecido para la respuesta a incidentes de seguridad de la información * Existe la iniciativa para la detección de riesgos por la Unidad de Riesgos de la organización, pero no hay proceso de planificación y preparación de la gestión de incidentes de Seguridad Informática	1

A5.27	Aprender de los incidentes de seguridad de la información	**Control** Los conocimientos adquiridos en los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.	* No hay un plan de mejora establecido en relación a las experiencias previas de incidentes de información que hayan sido detectados y mitigados	1
A5.28	Obtención de pruebas	**Control** La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	* No existe un proceso forense para la obtención de pruebas * No se ha establecido una cadena de custodia en caso de ser requerido en un delito informático	1
A5.29	Seguridad de la información durante la interrupción	**Control** La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	* Existe un plan de contingencia para las interrupciones de servicios más generales que podrían llegar a suscitarse	3
A5.30	Preparación de las TIC para la continuidad de las actividades	**Control** La preparación para las TIC se planificará, aplicará, mantendrá y probará sobre la base de los objetivos de continuidad de las actividades y los requisitos de continuidad de las TIC.	* Existe un plan de continuidad de negocio, así como plan de contingencia para hacer frente a las eventualidades más conocidas en el entorno de sistemas	3
A5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	**Control** Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.	* Reconocimiento de existencia de leyes en materia de Tecnologías de la Información, algunos de estos han sido retomados dentro de la política, pero no se han establecido el cumplimiento requerido por parte de la cooperativa	1
A5.32	Derechos de propiedad intelectual	**Control** La organización aplicará procedimientos apropiados para proteger los derechos de propiedad intelectual.	* Definido dentro del manual de gestión de riesgos tecnológico * Establecido dentro de la política de información	3

A5.33	Protección de registros	**Control** Los registros estarán protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	* Plan de contingencia en caso de pérdida * Backups periódicos en formato digital y físico. De igual forma alojados en ubicaciones externas a la organización (nube de datos privadas) * Algunos almacenes para guardado de copias físicas son compartidos, resulta de vital importancia poseer un espacio único y con acceso únicamente por personal previamente definido para asegurar la disponibilidad e integridad de las copias y respaldo	3
A5.34	Privacidad y protección de la información de identificación personal (PII)	**Control** La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de Pll de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.	* No hay una política de protección de datos que se pueda evaluar o se evidencia iniciativa para la creación de la misma	0
A5.35	Examen independiente de la seguridad de la información	**Control** El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.	* Son evaluadas de forma general mediante auditorias * No se muestran evidencias de evaluación de buenas prácticas o cumplimientos de normas técnicas de seguridad	2
A5.36	Cumplimiento de políticas, reglas y estándares para la seguridad de la información	**Control** El cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos del tema se revisarán regularmente.	* Hay evidencia de auditorías que se realizan de forma periódica, pero estas se enfocan más en la parte documental que el carácter técnico	2
A5.37	Procedimientos operativos documentados	**Control** Los procedimientos operativos de las instalaciones de tratamiento de la información se documentarán y se pondrán a disposición del personal que los necesite.	* Mayoría de procedimientos se encuentra definidos en la política y manuales * La actualización de dichos documentos no es periódica, no existe tampoco evidencias de mejora continua sobre los mismos * Mayoría de documentos no han sido	3

			publicados de forma oportuna para el conocimiento de toda la cooperativa	
A.6 Controles de personas				**3**
A6.1	Chequeo	**Control** Las verificaciones de antecedentes de todos los candidatos a convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.	* Por ser una entidad financiera se realizan diversos chequeos de antecedentes como: policiales, penitenciarios, score crediticio y pruebas de personalidad y conocimientos para poder ser tomados en cuenta para una plaza determinada dentro de la cooperativa	4
A6.2	Términos y condiciones de empleo	**Control** Los acuerdos contractuales de empleo establecerán las responsabilidades del personal y de la organización para la seguridad de la información.	* Se han establecido perfiles de los puestos relacionados a TI, así como el conocimiento requerido, responsabilidades y funciones que estos deberán realizar como parte de su rol dentro de la cooperativa	3
A6.3	Concienciación, educación y capacitación sobre seguridad de la información	**Control** El personal de la organización y las partes interesadas pertinentes recibirán concienciación, educación y capacitación apropiadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.	* El personal de la cooperativa recibe concientización y capacitaciones sobre seguridad de la información, pero no hay evidencia de que la política de seguridad se actualizada periódicamente.	3
A6.4	Proceso disciplinario	**Control** Se formalizará y comunicará un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.	* En la política de seguridad no se menciona las sanciones impuestas contra el personal y las partes interesadas que hace referencia al proceso disciplinario aplicable ante la violación de la política.	3

A6.5	Responsabilidades después de la terminación o cambio de empleo	**Control** Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o cambio de empleo se definirán, harán cumplir y comunicarán al personal pertinente y otras partes interesadas.	* Se comunican los deberes de la información que siguen siendo validos después de la terminación o cambio de empleo.	3
A6.6	Acuerdos de confidencialidad o no divulgación	**Control** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización en materia de protección de la información serán identificados, documentados, revisados periódicamente y firmados por el personal y otras partes interesadas pertinentes.	* Están definidos y documentados los acuerdos de confiablidad o no divulgación.	3
A6.7	Trabajo remoto	**Control** Las medidas de seguridad se implementarán cuando el personal trabaje de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.	* Se implementan VPN como medida de seguridad para las conexiones remotas para proteger la información a la que se accede.	3
A6.8	Informes de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados de manera oportuna.	* Deben la cooperativa implementar y establecer canales, mecanismos para que el personal informe eventos de seguridad.	2
A.7 Controles físicos				**4**
A7.1	Perímetros de seguridad física	**Control** Los perímetros de seguridad se definirán y utilizarán para proteger las zonas que contengan información y otros activos asociados.	* Se protegen los perímetros y zonas que contienen información y activos.	5

A7.2	Entrada física	**Control** Las zonas seguras estarán protegidas por controles de entrada y puntos de acceso adecuados. Las zonas seguras estarán protegidas por controles de entrada y puntos de acceso adecuados.	* Las zonas seguras están protegidas por controles de entrada y puntos de accesos adecuados.	5
A7.3	Asegurar oficinas, habitaciones e instalaciones	**Control** Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.	* Se aplica seguridad física en las oficinas, salas e instalaciones ya que es un banco y por rigor aseguran las instalaciones.	5
A7.4	Monitoreo de seguridad física	**Control** Los locales serán monitoreados continuamente para detectar el acceso físico no autorizado.	* Continuamente los accesos físicos son monitoreados 24/7. * El monitoreo debe ser gestionado por la seguridad y centralizado.	3
A7.5	Protección contra amenazas físicas y ambientales	**Control** Se diseñará y aplicará la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionales a las infraestructuras.	* Se aplica protección contra amenazas físicas y medioambientales para asegurar la infraestructura.	5
A7.6	Trabajar en zonas seguras	**Control** Se diseñarán y aplicarán medidas de seguridad para trabajar en zonas seguras.	* Se aplican medidas de seguridad para trabajar en zonas seguras.	3
A7.7	Escritorio claro y pantalla clara	**Control** Se definirán y aplicarán adecuadamente normas de escritorio claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas para las instalaciones de tratamiento de la información.	* Se han definido normas claras para el tratamiento de la información, pero los usuarios pueden no ser conscientes de sus responsabilidades.	2
A7.8	Escritorio claro y pantalla clara	**Control** El equipo deberá estar colocado de forma segura y protegida.	* Los equipos están colocados de forma segura.	4

A7.9	Seguridad de los activos fuera de las instalaciones	**Control** Los activos externos estarán protegidos.	* Existe protección externa para los activos	3
A7.10	Medios de almacenamiento	**Control** Los medios de almacenamiento se gestionarán durante todo su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	* Los medios de almacenamiento se gestionarán durante todo su ciclo de vida de adquisición	3
A7.11	Utilidades de apoyo	**Control** Las instalaciones de tratamiento de la información deberán estar protegidas contra fallos de suministro eléctrico y otras interrupciones causadas por fallos en los servicios públicos de apoyo.	* Existe protección contra fallos de suministro eléctricos y fallos de servicios públicos.	5
A7.12	Seguridad del cableado	**Control** Los cables que transporten energía, datos o servicios de información de apoyo estarán protegidos contra interceptaciones, interferencias o daños.	* Los cables de datos y servicios de información están protegidos contra interferencias y daños.	5
A7.13	Mantenimiento de equipos	**Control** El equipo deberá mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	* Se garantiza la disponibilidad, integridad y confidencialidad de la información.	4
A7.14	Eliminación segura o reutilización del equipo	**Control** Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	* Se verifica la eliminación segura en los equipos que contengan medios de almacenamiento para garantizar que los datos confidenciales	4
A.8 Controles tecnológicos				**3.56**

A8.1	Dispositivos de punto final de usuario	**Control** Se protegerá la información almacenada, tratada o accesible a través de dispositivos de punto final de usuario.	* La información almacenada accesible por dispositivos de punto final de usuario es protegida.	3
A8.2	Derechos de acceso privilegiados	**Control** Se restringirá y gestionará la asignación y el uso de derechos de acceso privilegiados.	* Se gestiona el uso de derechos de acceso y privilegios.	3
A8.3	Restricción de acceso a la información	**Control** El acceso a la información y otros activos asociados se restringirá de acuerdo con la política de control de acceso establecida sobre temas específicos.	* Se restringe el acceso a la información de acuerdo a la política de control de acceso.	3
A8.4	Acceso al código fuente	**Control** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.	* Se gestiona el acceso al código fuente.	3
A8.5	Autenticación segura	**Control** Las tecnologías y procedimientos de autenticación segura se implementarán sobre la base de las restricciones de acceso a la información y la política de control de acceso específica del tema.	* Se implementa la autenticación segura para restringir el acceso a la información.	4
A8.6	Gestión de la capacidad	**Control** El uso de los recursos se supervisará y ajustará en función de las necesidades de capacidad actuales y previstas.	* Se gestiona la capacidad, se supervisa y ajusta de acuerdo a las necesidades.	4
A8.7	Protección contra malware	**Control** La protección contra el malware se implementará y estará respaldada por un conocimiento adecuado del usuario.	* Se implementa protección contra malware y está respaldada por un conocimiento adecuado del usuario.	4

A8.8	Gestión de vulnerabilidades técnicas	**Control** Se obtendrá información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas apropiadas.	* Se tiene definido en la política la forma de gestionar las vulnerabilidades que se puedan presentar en los sistemas de información y dar solución de manera efectiva.	3
A8.9	Gestión de la configuración	**Control** Se establecerán, documentarán, aplicarán, supervisarán y revisarán las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes.	* En la política se establece la documentación necesaria para las configuraciones en seguridad que deben tener los dispositivos activos. * Cambiar y omitir las configuraciones por default.	4
A8.10	Eliminación de información	**Control** La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.	* según política establecida, se debe realizar procedimiento para eliminar la información que no se utilice, debe ser destruida para evitar que pueda ser manipulada.	4
A8.11	Enmascaramiento de datos	**Control** El enmascaramiento de datos se utilizará de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas específicas de temas relacionados, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.	* No se tiene una persona encargada de realizar los enmascaramientos en los datos, para controlar los accesos.	4
A8.12	Prevención de fuga de datos	**Control** Se aplicarán medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	* Se deben realizar controles para la manipulación de los datos, ¨Se debe tener medidas de seguridad para evitar la fuga de la emisión.	3
A8.13	Copia de seguridad de la información	**Control** Las copias de seguridad de la información, los programas informáticos y los sistemas se mantendrán y probarán periódicamente de conformidad con la política acordada sobre copias de seguridad sobre temas específicos.	* Se deben tener procedimientos para realizar los respaldos de los datos y de toda la información, sea de usuarios, servidores y dispositivos activos.	4

A8.14	Redundancia de instalaciones de procesamiento de información	**Control** Las instalaciones de tratamiento de la información se implantarán con una redundancia suficiente para cumplir los requisitos de disponibilidad.	* Se tiene redundancia en las instalaciones para el manejo de la información, de forma local y en la nube, que forma parte de la redundancia.	4
A8.15	Registro	**Control** Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallos y otros eventos relevantes.	* Según política se deben realizar registros de las actividades, pero no se tiene una persona encargada y que se oriente a ver dichos registros, para su respectivo análisis.	3
A8.16	Actividades de supervisión	**Control** Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se tomarán las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.	* No se tiene una persona especializada en seguridad de la información, para realizar la supervisión de los sistemas, aplicaciones y redes, que le permita detectar anomalías y se puedan tomar medidas de seguridad.	3
A8.17	Sincronización del reloj	**Control** Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.	* Se tienen sincronizados los relojes de los sistemas en los servidores. * En la política se maneja que el servidor de dominio debe dar el servicio para que los equipos clientes estén sincronizados.	3
A8.18	Uso de programas de utilidad privilegiados	**Control** El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.	* Se tienen programas para el control del sistema y de aplicaciones, pero hace falta un especialista de la seguridad de la información que realice las restricciones. * Según política está definido que se debe controlar y restringir programas que no sean parte de la cooperativa asimismo ser controlados.	4
A8.19	Instalación de software en sistemas operativos	**Control** Se implementarán procedimientos y medidas para administrar de forma segura la instalación de software en los sistemas operativos.	* No hay control de los programas o software a instalar en los equipos, asimismo procedimiento y controles que permitan o denieguen según la autorización.	4

A8.20	Seguridad de redes	**Control** Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.	* Hace falta tener un especialista para que pueda dar seguimiento, gestionar y administrar los dispositivos activos.	4
A8.21	Seguridad en los servicios de red	**Control** Se identificarán, aplicarán y supervisarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.	* No existe el especialista que pueda gestionar los controles en seguridad de la información, los niveles de servicio y puedan ser gestionados en todos los servicios de la red.	4
A8.22	Segregación de redes	**Control** Los grupos de servicios de información, usuarios y sistemas de información se separarán en las redes de la organización.	* Según la política se hace segregación de las redes para seguridad de servicios, usuarios y sistemas.	4
A8.23	Filtrado web	**Control** El acceso a sitios web externos se gestionará para reducir la exposición a contenidos maliciosos.	* Por políticas es prohibido el acceso a sitios externos no seguros y contenido malicioso, se realiza filtrado web.	4
A8.24	Uso de criptografía	**Control** Se definirán y aplicarán normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.	* De acuerdo a política se aplica criptografía a la información y se gestionan las claves criptográficas.	4
A8.25	Ciclo de vida de desarrollo seguro	**Control** Se establecerán y aplicarán normas para el desarrollo seguro de programas informáticos y sistemas.	* Por política de la cooperativa y procedimientos de TIC se aplican normas para desarrollar de forma segura aplicaciones y mejoras al software.	3
A8.26	Requisitos de seguridad de las aplicaciones	**Control** Los requisitos de seguridad de la información se identificarán, especificarán y aprobarán al desarrollar o adquirir aplicaciones.	* Por políticas y procedimientos establecidos, se realizarán requisitos y/o requerimientos con seguridad, para el desarrollo de las aplicaciones y/o mejoras al software.	4

A8.27	Requisitos de seguridad de las aplicaciones	**Control** Los principios para la ingeniería de sistemas seguros se establecerán, documentarán, mantendrán y aplicarán a cualquier actividad de desarrollo de sistemas de información.	* Se han establecido en la política que se realice la documentación necesaria por los requisitos y/o requerimientos que se han desarrollo en las aplicaciones y/o software.	4
A8.28	Codificación segura	**Control** Los principios de codificación segura se aplicarán al desarrollo de software.	* En la política se manifiesta que deben realizar código de forma segura, en desarrollo de software y aplicaciones.	3
A8.29	Pruebas de seguridad en desarrollo y aceptación	**Control** Los procesos de pruebas de seguridad se definirán y aplicarán en el ciclo de vida del desarrollo.	* En la política se menciona que deben realizar que se deben realizar pruebas en el desarrollo de software y aplicaciones, así como de aceptación.	3
A8.30	Desarrollo externalizado	**Control** La organización dirigirá, supervisará y revisará las actividades relacionadas con el desarrollo de sistemas subcontratados.	* Se siguen procedimientos de forma segura para el desarrollo de software y aplicaciones que son subcontratados.	3
A8.31	Separación de entornos de desarrollo, prueba y producción	**Control** Los entornos de desarrollo, ensayo y producción deberán estar separados y protegidos.	* Tienen los diferentes ambientes para el desarrollo de aplicaciones y sistemas.	3
A8.32	Gestión del cambio	**Control** Los cambios en las instalaciones de tratamiento de la información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.	* Planifican los cambios que se van a realizar en las instalaciones del datacenter, a las aplicaciones y sistemas.	4
A8.33	Información de la prueba	**Control** La información del ensayo se seleccionará, protegerá y gestionará adecuadamente.	* Seleccionan la información para las pruebas a realizar en los sistemas. * Realizar pruebas basadas en procedimientos. * Tienen ambiente de pruebas para realizarlas. * Deben tener un especialista QA para revisión de pruebas y calidad.	3

A8.34	Protección de los sistemas de información durante las pruebas de auditoría	**Control** Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se planificarán y acordarán entre el evaluador y la dirección apropiada.	* Tienen auditorías a los sistemas de la cooperativa. * Realizan monitoreo de los sistemas.	4

Análisis de Resultados

La Cooperativa SIHUACOOP DE R.L. se encuentra clasificada en un nivel global 3.88 en los controles A5, A6, A7 y A8 de la norma ISO 27001:2022. Lo cual no es del todo malo, dado que existen evidencias de muchos procesos que se han trabajo de forma razonable, pero hay otros que no están respaldados por políticas o controles que enfuercen la utilización en todos los niveles de la organización, esto es definitivamente un punto que debe ser mejorado.

De igual forma, existen otros controles con nula existencia siquiera de la iniciativa de mejora, recomendamos que se evalúen en su totalidad todos los controles establecidos en el Anexo A de la norma ISO 27001.

Tabla 6565.Resultado evaluación por nivel y global.

Control	Nivel
A.5 Controles Organizacionales	2
A.6 Controles de personas	3
A.7 Controles físicos	4
A.8 Controles tecnológicos	3.55
NIVEL GOBAL	**3.88**

Nivel actual de MMC de cada área de control de seguridad de ISO 27001:2022 Anexo A

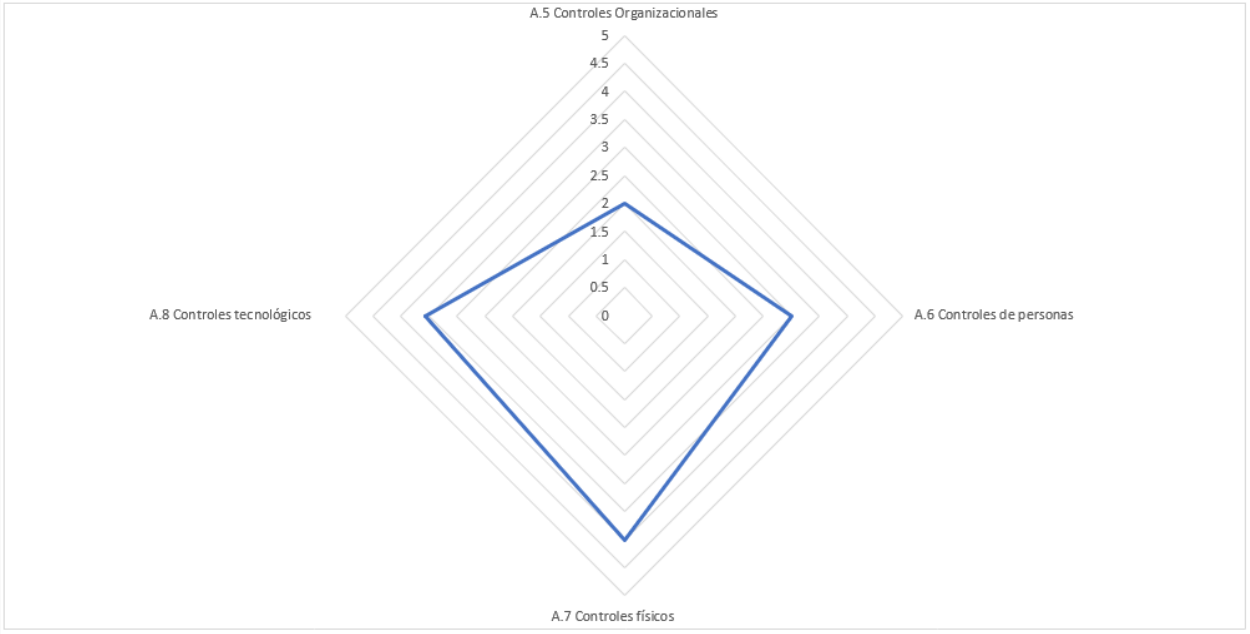


Ilustración 9 resultados evaluación controles ISO 27001:2022

Como podemos apreciar en la Ilustración 4, el control A.5 Controles Organizacionales, es el control con menos nivel de implementación. Lo cual tiene sentido dado que la mayoría de los procesos han sido manejados hasta ahora bajo buenas prácticas, si aplican y procesos ad-hoc.

Se deben de subsanar las observaciones detalladas en el informe de auditoría y evaluar nuevamente estos controles, recomendamos además evaluar la totalidad de controles de la norma ISO 27001, con fin de crear un SGSI robusto y escalable a largo plazo.

Beneficios

Los beneficios que se pueden obtener al implementar un SGSI propuesto por la Norma internacional ISO27001:2023 son muchos listaremos los más relevantes según nuestro criterio.

- ✓ Interoperabilidad
  Se trata de una ventaja general de la normalización. La idea es que los sistemas de diversas partes tienen más probabilidades de encajar entre sí si siguen una directriz común.

- ✓ Garantía
  La dirección puede estar segura de la calidad de un sistema, unidad de negocio u otra entidad si se sigue un marco o enfoque reconocido.

- ✓ Diligencia debida
  El cumplimiento de una norma internacional, o la certificación con arreglo a la misma, suele ser utilizado por la dirección para demostrar la diligencia debida.

- ✓ Evaluación comparativa
  Las organizaciones suelen utilizar una norma como medida de su estatus dentro de su comunidad de pares. Puede utilizarse como punto de referencia para la posición actual y el progreso.

- ✓ Concienciación
  La aplicación de una norma como la ISO 27001 puede dar lugar a una mayor concienciación en materia de seguridad dentro de una organización.

- ✓ Alineación

  Debido a que la aplicación de la norma ISO 27001 (y las otras normas ISO 27000) tiende a involucrar tanto a la gestión empresarial como al personal técnico, a menudo resulta en una mayor alineación de TI y de negocios.

- ✓ Conformidad

  Si una organización debe cumplir varias normativas relativas a la protección de datos, la privacidad y el gobierno de TI (especialmente si se trata de una organización financiera, sanitaria o gubernamental), la norma ISO 27001 puede aportar la metodología que permita hacerlo de la forma más eficaz.

- ✓ Ventaja comercial

  En un mercado cada vez más competitivo, a veces es muy difícil encontrar algo que le diferencie a los ojos de sus clientes. La norma ISO 27001 podría ser un argumento de venta único, especialmente si maneja información confidencial de sus clientes.

- ✓ Reducción de gastos

  La seguridad de la información suele considerarse un coste sin beneficios económicos evidentes. Sin embargo, existe un beneficio financiero si reduce los gastos causados por incidentes. Probablemente tenga una interrupción del servicio, o una fuga de datos ocasional, o empleados descontentos. O antiguos empleados descontentos. La verdad es que aún no existe una metodología y/o tecnología para calcular cuánto dinero podría ahorrar si evitara esos incidentes. Pero siempre suena bien llamar la atención de la dirección sobre estos casos.

- ✓ Poner orden en la empresa

  Esta es probablemente la más infravalorada. Si eres una empresa que ha crecido mucho en los últimos años, es posible que tengas problemas como: quién tiene que decidir qué, quién es responsable de determinados activos de información, quién tiene que autorizar el acceso a los sistemas de información, etc.

Conclusiones

Se llevó a cabo un análisis preliminar de ciertos aspectos seleccionados por su relevancia en el funcionamiento del negocio. El objetivo primordial es asegurar la integridad de los recursos y activos de información de la organización, así como garantizar la calidad y seguridad de los servicios financieros proporcionados a los asociados a nivel nacional. Es fundamental destacar que el éxito de estas iniciativas depende en gran medida del total respaldo de las áreas de negocio, ya que el departamento por sí solo no puede introducir nuevas políticas y controles, a menos que cuente con el apoyo de las unidades a las que presta servicio de manera diaria.

Se ha llevado a cabo una evaluación exhaustiva de los elementos requeridos, basándose en las directrices de la norma ISO 27001:2022. Los resultados obtenidos serán aprovechados para obtener un análisis preliminar de la situación empresarial, con el propósito de definir la estrategia necesaria para la correcta implementación del Sistema de Gestión de Seguridad de la Información.

Recomendaciones

- SIHUACOOP DE R.L. ha comenzado un proceso que seguramente será de gran beneficio, sin embargo, recomendamos realizar una evaluación de todos los controles de norma ISO 27001:2022, a fin de lograr un SGSI robusto que sea mantenible a largo plazo y que este respaldado además por las altas direcciones.

- Existen muchos procesos que están basados en buenas prácticas, pero que no está documentados en políticas y procedimientos que faciliten la distribución y adopción de estos a diversos niveles de la organización. Se sugiere asegurar y esforzar que existan procedimientos claros que eliminen la ambigüedad y confusión al momento de ejecutar procesos, dichos procedimientos deben ser comunicados de forma amplia a toda la organización y niveles, respaldados por las áreas gerenciales y de dirección de la organización.

- Si bien es cierto, La Cooperativa SIHUACOOP DE R.L. ya estaba familiarizada con la ISO, recomendamos evaluar la posibilidad de implementar norma ISO 27001:2022 que además puede ser combinada con otras normas y/o marcos de trabajo como la norma ISO 27005. La idea es crear un sistema robusto, tomando las características que consideremos que se adapta de mejor forma a la organización, de tal forma que siempre se cumplan los requerimientos del negocio, usando los controles y beneficios que se consideren más adecuados para el ecosistema.

- Realizar evaluaciones de riesgos de forma trimestral a los activos que tenga la cooperativa, o cuando lo estime necesario y conveniente, para dar

seguimiento a los cambios que puedan surgir en las diferentes áreas/o agencias involucradas en toda la cooperativa.

- Se sugiere dar seguimiento de actualización a la política de seguridad de la información cada 6 meses o cuando sea necesario realizar una nueva versión de la política, siempre siguiendo los lineamientos de la cooperativa para su visto bueno, autorización y socialización con las áreas interesadas y colaboradores.

- En la evaluación y revisión se encontró que en el departamento de tecnología, hay una necesidad de personal para que puedan desempeñar de la mejor manera y eficiente las actividades, ya que el personal con el que se cuenta actualmente a falta de personal cubren otros puestos de trabajo que son necesarios para que no dejen desatendidos sus funciones y/o responsabilidades directas, se recomienda en la medida de lo posible se puedan asignar funciones principales y secundarias para los diferentes puestos de trabajo sugeridos en el área de seguridad de la información.

- Definir un sitio de contingencial físico en alguna de las sucursales para continuar las operaciones TI en caso se presente una catástrofe que imposibilite la operación de fallar la central.

- Implementar en la estructura organizativa un área de análisis de incidentes de seguridad SOC y de respuesta a estos.

- La video vigilancia no debe de ser una actividad de la Gerencia de TI, se debe de crear un proceso para persona de seguridad física se dedique al monitoreo de este circuito.

- Se aconseja contratar dos veces por año a una empresa especializada para que realice prueba de intrusión a la infraestructura tecnología y certificar la seguridad de la Cooperativa.

- Se recomienda realizar un plan para la normalización de las bases de datos.

- Se recomienda la expansión de la Gerencia de TI y garantizar la segregación de funciones.

- Se debe de establecer un plan de capacitación y concientización por lo menos 2 veces al año en materia de ciberseguridad a todo el personal de la cooperativa, no importando las funciones y puesto que este desempeñe.

Bibliografía

- Birchall, J. (2014). Reseña histórica del cooperativismo. Revista CIRIEC-España, (82), 9-42. doi: 10.7201/ciriec.2014.82.02
- García, A. (2015). El cooperativismo en El Salvador: Historia y actualidad. Revista de Economía y Derecho, (22), 97-110.
- Birchall, J. (2014). Reseña histórica del cooperativismo. Revista CIRIEC-España, (82), 9-42. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4765626
- Bishop, M. (2003). Computer security: Art and science. Pearson Education.
- Clarke, R. (1992). Information technology and dataveillance. Communications of the ACM, 35(9), 88-97. doi: 10.1145/129888.129893
- Denning, D. E. (1996). Cryptography and data security. Addison-Wesley Professional.
- Stallings, W. (2017). Cryptography and network security: Principles and practice. Pearson.
- ISO. (2021). What are ISO standards? Recuperado de https://www.iso.org/standards.html
- ISO. (2015). ISO 9001:2015 - Quality management systems - Requirements. Recuperado de https://www.iso.org/standard/62085.html
- ISO. (2018). ISO 14001:2015 - Environmental management systems - Requirements with guidance for use. Recuperado de https://www.iso.org/standard/60857.html
- ISO. (2018). ISO 45001:2018 - Occupational health and safety management systems - Requirements with guidance for use. Recuperado de https://www.iso.org/standard/63787.html
- ISO. (2013). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Recuperado de https://www.iso.org/standard/54534.html
- ISO. (2021). ISO survey 2020. Recuperado de https://www.iso.org/the-iso-survey.html
- Delgado, L. A., & Carvajal, J. A. (2017). Beneficios de la certificación en normas ISO en las pequeñas y medianas empresas. Revista Ciencias Estratégicas, 25(34), 91-99. Recuperado de https://www.redalyc.org/articulo.oa?id=41455332009

- ISO. (2021). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. Recuperado de https://www.iso.org/standard/54534.html
- Rezaei, S., & Khanmohammadi, M. (2020). Implementation of ISO/IEC 27001:2013 standard in small and medium enterprises (SMEs): A review. International Journal of Engineering and Advanced Technology (IJEAT), 9(3), 6443-6448. Recuperado de https://www.ijeat.org/wp-content/uploads/papers/v9i3/C6977029320.pdf
- Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2017). ISO 27001 ISMS framework for securing medical records management: A review. Future Internet, 9(2), 1-13. Recuperado de https://www.mdpi.com/1999-5903/9/2/20
- Arora, S., & Kumar, M. (2018). Benefits and challenges of implementing ISO 27001: A case study of an Indian organization. International Journal of Engineering and Technology, 7(4.28), 151-154. Recuperado de https://www.sciencepubco.com/index.php/ijet/article/view/22494
- Lasihua. (s.f.). Documentos SIHUACOOP. Recuperado de https://www.lasihua.com/documentos_sihuacoop.html
- Instituto Nacional de Fomento Cooperativo. (s.f.). Asociaciones Cooperativas. Recuperado de http://www.insafocoop.gob.sv/?page_id=268
- Asamblea Legislativa de la República de El Salvador. (s.f.). Ley General de Asociaciones Cooperativas. Recuperado de https://ssf.gob.sv/descargas/Leyes/Leyes%20Financieras/Ley%20General%20de%20Asociaciones%20Cooperativas.pdf
- Instituto Nacional de Fomento Cooperativo. (s.f.). Ley General de Asociaciones Cooperativas. Recuperado de https://www.insafocoop.gob.sv/?wpdmpro=ley-general-de-asociaciones-cooperativas
- Instituto Nacional de Fomento Cooperativo. (s.f.). Reformas al Reglamento General de Asociaciones Cooperativas. Recuperado de https://www.insafocoop.gob.sv/?wpdmpro=reformas-al-reglamento-general-de-asociaciones-cooperativas-2
- Instituto Nacional de Fomento Cooperativo. (s.f.). Reglamento General de Asociaciones Cooperativas. Recuperado de https://www.insafocoop.gob.sv/?wpdmpro=reglamento-general-de-asociaciones-cooperativas
- Lasihua. (s.f.). Estatutos SIHUACOOP. Recuperado de https://www.lasihua.com/pdf_s/estatutos-sihuacoop.pdf

- Asamblea Legislativa de El Salvador. (2015). Dictamen de la Comisión de Economía. Recuperado de https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/BE543A5B-398E-4606-9ED8-1927602AA121.pdf
- Asamblea Legislativa de El Salvador. (2019). Dictamen de la Comisión de Economía. Recuperado de https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/498798FA-A563-4830-A0C8-306AFBC71497.pdf
- Organismo de Supervisión del Sistema Financiero. (s.f.). Historia OSN. Recuperado de https://www.osn.gob.sv/institucion/marco-institucional/historia-osn/
- Coops4dev. (s.f.). El Salvador. Recuperado de https://coops4dev.coop/es/4devamericas/salvador
- Coops4dev. (2021). Informe de Marcos Legales - El Salvador. Recuperado de https://coops4dev.coop/sites/default/files/2021-03/Informe%20de%20Marcos%20Legales%20-%20El%20Salvador.pdf
- Asamblea Legislativa de El Salvador. (2017). Decreto Legislativo No. 254. Recuperado de https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf
- Instituto Salvadoreño de Fomento Cooperativo. (s.f.). Servicio 2. Recuperado de https://www.insafocoop.gob.sv/?servicios=servicio-2
- Informática Jurídica. (s.f.). Legislación El Salvador. Recuperado de https://www.informatica-juridica.com/legislacion/el-salvador/
- Transparencia Institucional. (s.f.). Ley principal que rige a la institución. Recuperado de https://www.transparencia.gob.sv/institutions/insafocoop/documents/ley-principal-que-rige-a-la-institucion
- Informática Jurídica. (s.f.). Decreto Legislativo No. 534. Recuperado de https://www.informatica-juridica.com/legislacion/anexos/Decreto_534_2_diciembre_2010_Ley_Acceso_Informacion_Publica.asp%20.asp
- Gobierno Electrónico. (2018). Leyes aplicables a Gobierno Electrónico. Recuperado de https://www.gobiernoelectronico.gob.sv/wp-content/uploads/2018/04/3.-Leyes-aplicables-a-Gobierno-Electr%C3%B3nico.pdf

- OTRS. (s.f.). Sistema de Gestión de Seguridad de la Información (SGSI). Recuperado de https://otrs.com/es/casos-de-uso/sgsi/#:~:text=SGSI%20es%20un%20Sistema%20de,que%20deben%20llevarse%20a%20cabo.
- Firma-e. (s.f.). ¿Qué es un SGSI (Sistema de Gestión de Seguridad de la Información)? Recuperado de https://www.firma-e.com/blog/que-es
- Organismo Salvadoreño de Normalización. (2021). ¿Quiénes somos? Recuperado el 25 de marzo de 2023, de https://www.osn.gob.sv/institucion/quienes-somos/
- Organismo Salvadoreño de Normalización. (2021). ISO 27001: Seguridad de la información. Recuperado el 25 de marzo de 2023, de https://www.osn.gob.sv/servicios/normas-de-sistemas-de-gestion/iso-27001-seguridad-de-la-informacion/
- DQS Certificación de Sistemas de Gestión. (s.f.). ISO 27001. https://www.dqsglobal.com/es-sv/frontend_search?q=ISO+27001
- Icontec. (s.f.). Certificación ISO 27001. https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2 /
- Norma ISO 27001. (s.f.). Fase 10: El proceso de certificación ISO 27001. https://normaiso27001.es/fase-10-el-proceso-de-certificacion-iso-27001/
- Entidad Nacional de Acreditación. (s.f.). ENAC. www.enac.es

Deloitte. (s.f.). Deloitte El Salvador. https://www2.deloitte.com/sv/es.html

https://www.informatica-juridica.com/ley/decreto-no-133-ley-de-firma-electronica-de-el-salvador/

https://www.csj.gob.sv/wp-content/uploads/2020/11/PARTE-1.Codigo-Penal_1890.pdf

Glosario

Activos: Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

Amenazas: Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

Gestión Del Riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

Impactos: Las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

ISO: (Internacional Organization for Standardization) es la **Organización Internacional de Normalización**, cuya principal actividad es la elaboración de normas técnicas internacionales.

ISO/IEC 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Norma: Describe los controles y las consideraciones de implementación, no especifica exactamente cómo debe hacerse. Es un documento público, consensuado por todas las partes interesadas y aprobado por un Organismo de Normalización reconocido.

SGSI: Sistema de Gestión de Seguridad de la Información, es un conjunto de principios o procedimientos que se utilizan para identificar riesgos y definir los pasos de mitigación de riesgos que deben llevarse a cabo.

Vulnerabilidad: Una vulnerabilidad es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Marco de trabajo: Es un conjunto de elementos de conceptos, prácticas, conocimientos, conceptos, entre otros. Tienen como finalidad ser aplicadas hacia una problemática.

Buenas Prácticas: Son aquellas pautas aconsejables que se adaptan a un determinado punto de vista de un proceso a realizar dentro de la empresa.

Políticas: Es un proceso para establecer norma para realizar los procedimientos adecuados dentro de las empresas.

Riesgo: Es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños.