

ISO 27001



Auditor Interno

**Seguridad de la información, ciberseguridad
y protección de la privacidad**

Copyright and Disclaimer

Copyright © T-CERT

Miami, Florida

2024

Todos los derechos reservados.

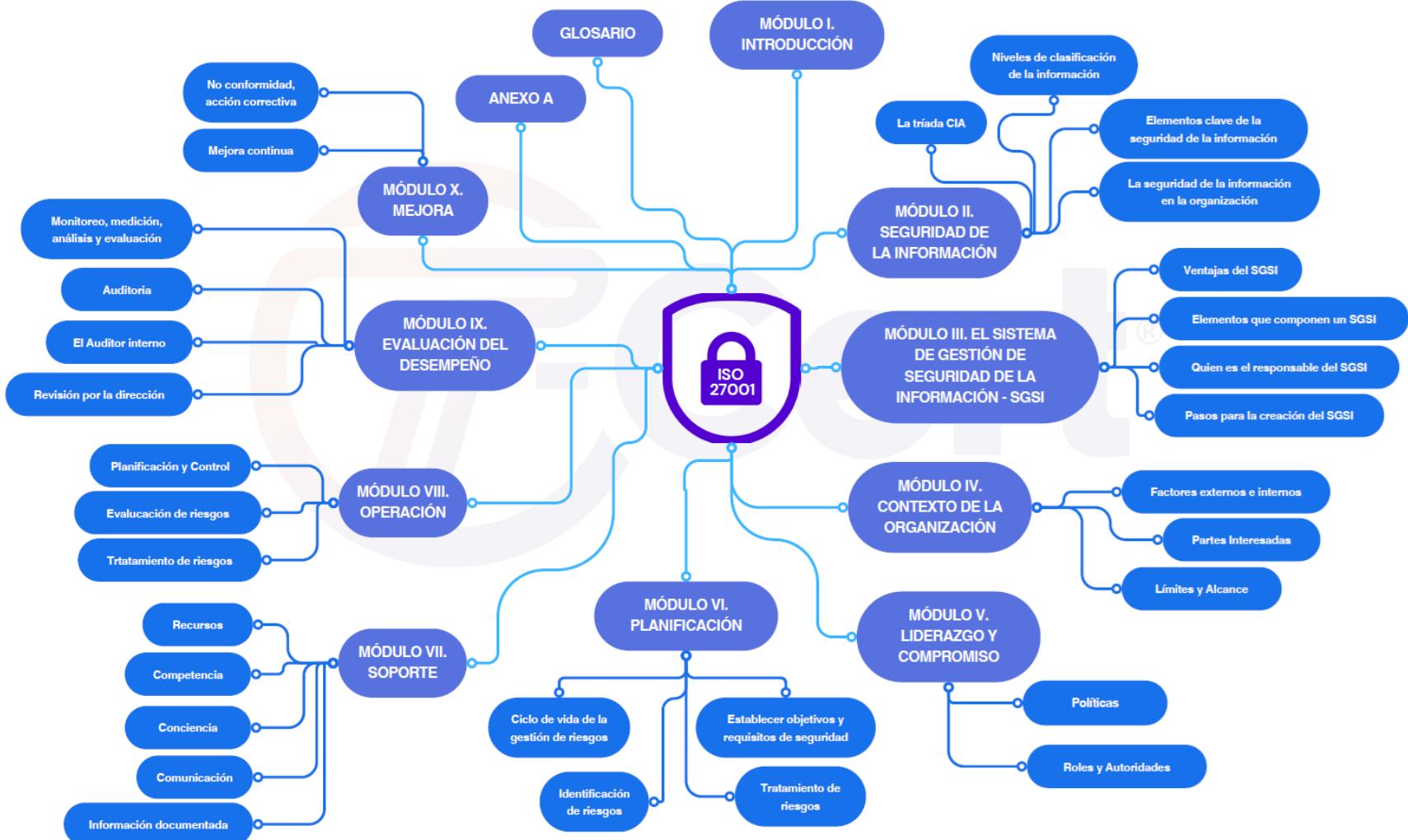
Ninguna parte de esta publicación puede reproducirse, de ninguna forma y por ningún medio, sin el permiso por escrito de T-CERT.

Esta es una publicación comercial confidencial. Todos los derechos reservados. Este documento no puede ser copiado, reproducido en parte, reproducido, traducido, fotocopiado o reducido a cualquier medio sin el consentimiento previo y expreso por escrito del editor. Este curso incluye trabajos sujetos a derechos de autor bajo licencia y está protegido por los derechos de autor

Disclaimer

La información proporcionada sobre el curso, los módulos, los temas y cualquier servicio para los cursos, incluyendo simulaciones o folletos, son sólo una expresión de intenciones y no deben tomarse como una oferta firme o compromiso.

Agenda



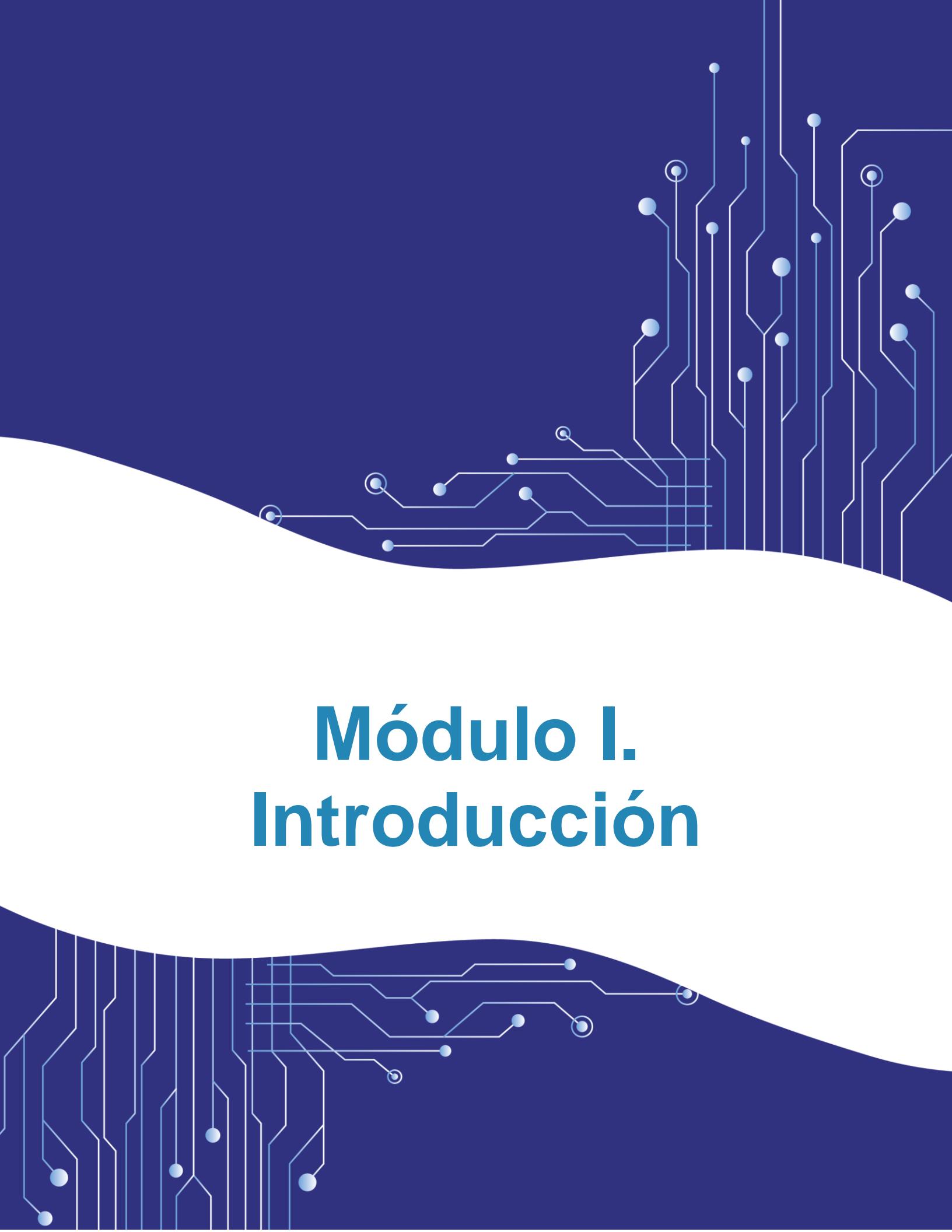
Contenido

Pág.

Módulo I. Introducción.....	8
1.1. Familia ISO 27000	8
1.2. ISO/IEC 27001	8
1.2.1. ¿Qué es la norma ISO/IEC 27001?	8
1.2.2. Estructura de la ISO/IEC 27001	9
1.2.3. ¿Por qué es importante la norma ISO/IEC 27001?	12
1.2.4. ¿Cómo funciona la norma ISO/IEC 27001?	13
1.2.5. ¿Quién necesita la norma ISO/IEC 27001?	13
1.2.6. ¿Cómo contribuirá la norma ISO/IEC 27001 a la organización?	14
Módulo II. Seguridad de la Información.....	16
2.1. La tríada CIA.....	16
2.2. Niveles de clasificación de la información	18
2.3. Elementos clave de la seguridad de la información.....	20
2.4. La seguridad de la información en la organización.....	21
Módulo III. El Sistema de Gestión de Seguridad de la Información – SGSI....	24
3.1. Ventajas del SGSI.....	24
3.2. Elementos que componen un SGSI	26
3.3. Quien es el responsable del SGSI	27
3.4. Pasos para la creación del SGSI	28
Módulo IV. Contexto de la Organización	31
4.1. Factores externos e internos.....	31
4.1.1. Modelo PESTEL	32
4.1.2. Análisis FODA	33
4.2. Partes interesadas	35
4.3. Límites y Alcance	36
4.3.1. Consideraciones antes de definir el Alcance del SGSI.....	37
4.3.2. Cómo definir el alcance de un SGSI	39
4.3.3. ¿Por qué definir el alcance del SGSI?	41
Módulo V. Liderazgo y Compromiso	43
5.1. Políticas	45
5.1.1. Puntos clave en la estructura de la política	46
5.1.2. Pasos para la definición de la política	47
5.2. Roles y Autoridades	47

5.2.1.	Responsabilidades.....	49
Módulo VI. Planificación		52
6.1.	Ciclo de vida de la gestión de riesgos	53
6.2.	Identificación de riesgos.....	54
6.2.1.	Tipos de riesgos	55
6.2.2.	Clasificación de riesgos	55
6.3.	Tratamiento de riesgos	56
6.3.1.	El plan de tratamiento de riesgos	57
6.3.2.	La declaración de aplicabilidad – SOA (Statement of Applicability)	58
6.4.	Establecer objetivos y requisitos de seguridad.....	60
Módulo VII. Soporte		62
7.1.	Recursos.....	62
7.2.	Competencia.....	63
7.3.	Conciencia	65
7.4.	Comunicación	65
7.5.	Información documentada.....	65
Módulo VIII. Operación		68
8.1.	Planificación y control	68
8.1.1.	Control de cambios	68
8.2.	Evaluación de riesgos	69
8.2.1.	Identificar los activos de información	70
8.2.2.	Clasificar la información.....	70
8.2.3.	Evaluar la información	72
8.2.4.	Definir los controles	73
8.3.	Tratamiento de riesgos	74
Módulo IX. Evaluación del desempeño		76
9.1.	Monitoreo, medición, análisis y evaluación	77
9.1.1.	Optimizar los recursos.....	77
9.1.2.	Establecer metas	77
9.1.3.	Medir la efectividad del SGSI	77
9.2.	Auditoría	79
9.2.1.	Tipos de Auditoría.....	79
9.2.2.	Auditoría interna	80
9.2.2.1.	Criterios de Auditoría	81
9.2.2.2.	Requisitos de la auditoría	81
9.2.2.3.	El alcance de la auditoría.....	81
9.2.2.4.	Selección de los auditores	82
9.2.2.5.	Informar los resultados	82
9.3.	El auditor interno.....	82
9.4.	Revisión por la dirección	84

Módulo X. Mejora	88
10.1. No conformidad, acción correctiva.....	88
10.1.1. Plan para la mejora	90
10.1.1.1. Paso 1: Registre todo lo que sea posible	90
10.1.1.2. Paso 2: Investigar y comunicarse	91
10.1.1.3. Paso 3: Aborde las no conformidades	91
10.1.1.4. Paso 4: Documente las evidencias	92
10.2. Mejora continua	93
Anexo A	99
1. A5 Controles Organizacionales	99
2. A6 Controles Orientados a las Personas	100
3. A7 Controles Físicos	101
4. A8 Controles Tecnológicos	102
Glosario	105



Módulo I.

Introducción

Módulo I. Introducción

1.1. Familia ISO 27000

La familia de normas para el SGSI se integra de:

- ISO 27000: Términos y vocabulario
 - 27001: Requisitos SGSI.
 - 27002: Guía de Implementación de controles.
 - 27003: Guía de Implementación SGSI.
 - 27004: Métricas SGSI.
 - 27005: Gestión de Riesgo de Seguridad de la Información.
 - 27006: Requisitos organismos de auditoría.

1.2. ISO/IEC 27001

1.2.1. ¿Qué es la norma ISO/IEC 27001?

La norma ISO (Organización Internacional de Normalización) / IEC (International Electrotechnical Commission) 27001 es la norma más conocida del mundo para Sistemas de Gestión de la Seguridad de la Información (SGSI o ISMS por sus siglas en inglés - Information Security Management System).

Esta norma, proporciona a empresas de cualquier tamaño, sector (público o privado) o industria, los controles para establecer, implantar, mantener y mejorar continuamente un SGSI. Con el fin, de que las organizaciones puedan gestionar efectivamente los riesgos, protegiendo la confidencialidad, la integridad y la disponibilidad de la información.



La certificación ISO/IEC 27001 es una forma de demostrar a las partes interesadas y a los clientes, que la organización está comprometida y puede gestionar la información de forma segura.

La ISO/IEC 27001 establece los objetivos que debe cumplir una organización para obtener la certificación. La certificación ISO/IEC 27001 en una empresa u organización significa que esta, ha implantado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que tiene o maneja, y que este sistema respeta los objetivos establecidos y las buenas prácticas de la norma.

NOTA: La certificación ISO/IEC 27001 es posible, pero NO ES OBLIGATORIA

1.2.2. Estructura de la ISO/IEC 27001

La norma tiene una estructura de alto nivel, que se divide en varias secciones, del 4 al 10 son requisitos obligatorios y el Anexo A, que hace referencia a los 93 controles de seguridad de la información. La norma Incluye:





1. Alcance

Alcance: Detalla la importancia de la norma y establece los límites de la aplicación del SGSI de una organización. Incluyendo la identificación de los activos de información que están cubiertos por la norma, las actividades y los procesos.



2. Referencias normativas

Referencias normativas: Hace referencia a otras normas internacionales de seguridad de la información, leyes de privacidad y protección de datos y otros marcos de seguridad de la información, que deben ser consideradas en el diseño, implementación y mantenimiento del SGSI.



3. Términos y definiciones

Términos y definiciones: Establece definiciones claras de los términos y conceptos clave utilizados en la norma para garantizar una comprensión común de los requisitos.



4. Contexto de la organización

Contexto de la organización: Detalla las indicaciones para entender a la organización, incluyendo su estructura y objetivos, además plantea la comprensión de las necesidades y expectativas de las partes interesadas. Esto, ayuda a identificar y evaluar los riesgos y oportunidades relevantes para un SGSI dentro de la organización.

Este es uno de los requisitos más importantes de la norma.



5. Liderazgo y compromiso

Liderazgo y compromiso: Establece los requisitos de liderazgo y compromiso de la alta gerencia para el SGSI. Esto incluye la elaboración y comunicación de la política de seguridad de la información, la asignación de roles y responsabilidades, además del establecimiento de objetivos y planes de mejora continua.

Planificación: Describe los requisitos para planificar el SGSI.

La organización debe identificar y evaluar los riesgos y oportunidades, además debe definir los objetivos y requisitos de seguridad y la forma en cómo se lograrían. Esto, incluye la selección de controles de seguridad y la elaboración de planes de implementación.



6. Planificación



7. Soporte

Soporte: Define los requisitos necesarios para implementar y mantener el SGSI. Para el buen funcionamiento del SGSI la organización debe contar con los recursos, la infraestructura y los recursos financieros. Así como también los requisitos para la competencia, la toma de conciencia y la comunicación e información documentada.



8. Operación

Operación: Indica los requerimientos para la planificación, la implementación y el control de los procesos de la organización. Se incluyen requisitos para la gestión de riesgos, la seguridad de la información, la documentación y el control de seguridad y accesos.



9. Evaluación del desempeño

Evaluación del desempeño: Establece los requisitos para llevar a cabo la medición, el seguimiento, el análisis, la evaluación, la realización de auditorías internas y las revisiones de gestión y evaluaciones del desempeño del SGSI.

Mejora: La organización tiene la responsabilidad de generar una cultura que se centre en la importancia de mejorar continuamente para la adecuación y eficacia del SGSI.



10. Mejora

Los 93 controles de la norma (Anexo A), están agrupados en 4 tipos de controles:

ANEXO A



1. Controles organizacionales



2. Controles de personal



3. Controles físicos



4. Controles tecnológicos

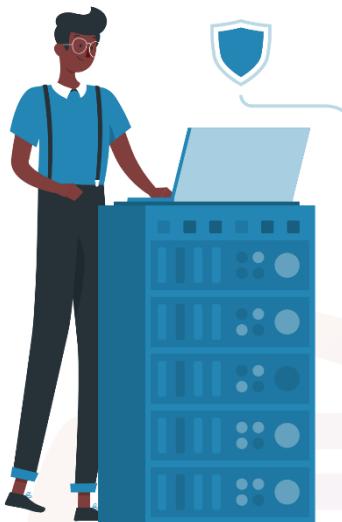
1.2.3. ¿Por qué es importante la norma ISO/IEC 27001?

Los avances tecnológicos a nivel mundial han incrementado las actividades de los ciberdelincuentes, haciendo que aparezcan amenazas constantemente, por lo que la gestión de estos riesgos puede parecer difícil.

La norma ISO/IEC 27001, promueve un enfoque holístico que ayuda a las organizaciones a ser más conscientes de los riesgos a los que se enfrenta su

información. Al mismo tiempo, ayuda a la identificación de los puntos débiles en la seguridad de la información en las personas, las políticas y la tecnología.

1.2.4. ¿Cómo funciona la norma ISO/IEC 27001?



La ISO/IEC 27001 es una forma de seguridad de información que busca proteger la privacidad e integridad de la información que tiene o maneja la organización, sin importar su tamaño.

Para lograr esto, la norma ISO/IEC 27001 cuenta con una estructura que ayuda a las organizaciones a identificar sus vulnerabilidades y riesgos a través de una evaluación, para así precisar la mitigación de estos, apoyándose en la definición de políticas y procedimientos.

1.2.5. ¿Quién necesita la norma ISO/IEC 27001?

Las empresas deben pensar en sus necesidades frente a la seguridad de la información y, en cómo estas se relacionan con sus objetivos y procesos. Si bien es cierto, en la actualidad la información es vulnerable y está expuesta a diferentes tipos de delitos. Por esta razón, las organizaciones deben tener un plan para prevenir cualquier riesgo que exponga sus datos.

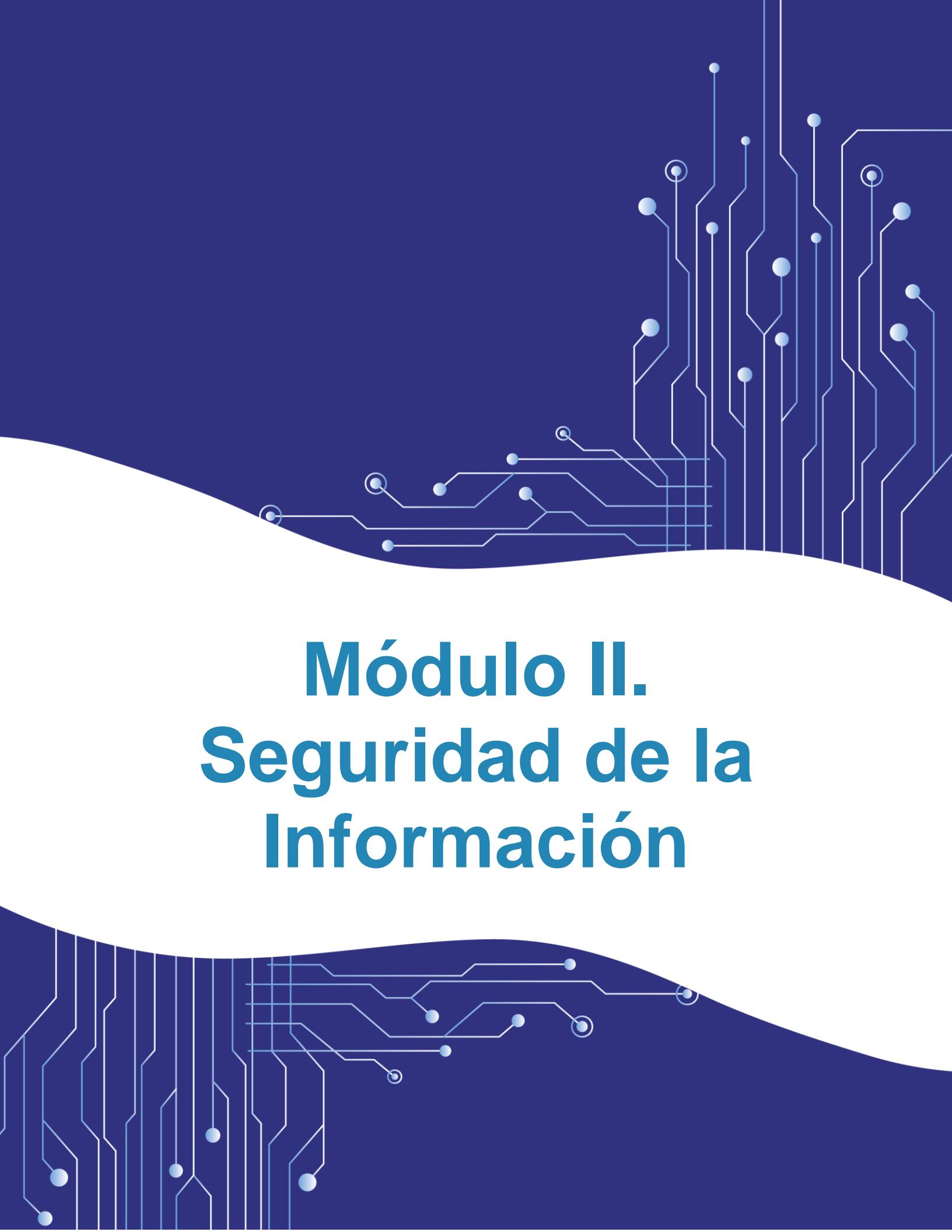
La norma ISO/IEC 27001 permite a las organizaciones construir un Sistema de Gestión de la Seguridad de la Información – SGSI y emplear un proceso de gestión de riesgos que se adapta a su tamaño y que puede modificarse según sus necesidades.

1.2.6. ¿Cómo contribuirá la norma ISO/IEC 27001 a la organización?

La implementación de la norma ISO/IEC 27001 para la seguridad de la información dentro de una organización, ayuda a:

- Reducir la vulnerabilidad ante ciberataques.
- Responder de forma efectiva a la transformación constante de los riesgos de seguridad.
- Garantizar que la información interna y externa de la organización se mantenga confidencial, integral y disponible cuando se requiera.
- Preparar a toda la organización desde las personas, los procesos y la tecnología para responder ante los riesgos tecnológicos y otras amenazas.
- Proteger la información en todas sus presentaciones, papel, digital y en la nube.





Módulo II.

Seguridad de la

Información

Módulo II. Seguridad de la Información

La seguridad de la información es un conjunto de operaciones y métodos, utilizados para proteger y controlar todos los datos que maneja una organización. Además, asegura los datos del uso indebido, accesos no autorizados, robo, interrupción o destrucción durante su ciclo de vida.

Este concepto comprende los aspectos desde la seguridad del hardware y los equipos de almacenamiento físicos, hasta los accesos entre dispositivos y ubicaciones, integrando las políticas y los procedimientos de la empresa.

La seguridad de la información comprende un conjunto de elementos que son clave para ayudar a proteger los datos de ciberataques, pero también de las amenazas internas y errores humanos. Estos elementos brindan mejoras a la organización en cuanto a la información confidencial y en como esta se usa.

2.1. La tríada CIA

Considerada como los tres pilares o principios fundamentales de la seguridad de la información, la tirada CIA reúne los esfuerzos y políticas de una organización para mantener seguros sus datos.





La Confidencialidad: Las organizaciones deben garantizar que solo las personas o usuarios autorizados tengan acceso a la información y que estos no se filtraran de ninguna forma.

Las estrategias que implementen las organizaciones en su sistema de seguridad de la información deben garantizar que la confidencialidad no se verá comprometida en ningún momento. Para lograr esto, existen herramientas como el cifrado, la autenticación en diferentes pasos y la precaución de perdida de datos.

La Integridad: Una buena gestión de la información debe garantizar la fiabilidad de la misma. Es decir que, esta debe mostrarse sin alteraciones o manipulaciones que no hayan sido evaluadas y autorizadas.

Se garantizará que la entrega de la información suministrada se encuentra en ambiente seguro, si se implementan protocolos seguros y técnicas que eviten riesgos. Para lograr esto, se pueden usar herramientas como administración de identidades, controles en los accesos y permisos de archivos.



Disponibilidad: Es importante que se garantice que la información estará disponible en todo momento para los sujetos autorizados, independiente de si es para su administración o de estricto conocimiento.

Para esto, se debe implementar un continuo mantenimiento de los equipos y la actualización del sistema, cuando sea necesario. Es decir que, la organización debe tomar medidas de soporte y seguridad que

garanticen que los usuarios dispongan de accesos fiables y coherentes a la información que requieran.

Sobre la triada CIA, cada organización debe establecer el cómo va a aplicar estos pilares, basándose en sus necesidades, objetivos y estructura, pero con el único fin de proporcionar a sus usuarios una experiencia segura.

2.2. Niveles de clasificación de la información

Existen 4 niveles de clasificación para la información con la que trabajan las organizaciones, independiente de su tamaño, actividad o sector. Estos, deben tenerse en cuenta para realizar una adecuada protección de los datos, estos niveles son:



1. Información Confidencial

La información confidencial, es la más crítica o la que es muy relevante para la organización, esta puede establecer los beneficios de la organización a mediano y largo plazo. Esta información es indispensable para un mejor funcionamiento de la organización y de sus operaciones. Conocer esta información ayudara a establecer las medidas de seguridad necesarias para su protección.

2. Información Restringida

La información restringida, es la que solo algunos integrantes de la organización tienen acceso. La clasificación de información en este punto tiene un componente subjetivo, ya que depende de la actividad o sector, para que los datos sean clasificados tan valiosos como para restringirlos.

3. Información Interna

Esta información, como su nombre lo indica, es la que se maneja solo dentro de la organización, esta información tiende a ser sensible, ya que puede representar información privada de clientes. Razón por la que se considera que, solo deben tener acceso a esta las mismas personas previamente autorizadas. La organización debe garantizar que sus sistemas de seguridad de información mantendrán la protección de los datos de las partes interesadas.



4. Información Pública

Esta información es de acceso público, es decir que cualquier persona dentro o fuera de la organización puede visualizar.

No toda la información y datos tienen el mismo valor. La organización debe clasificar esta información, posiblemente con un análisis interno con cada área que pueda determinar el nivel para cada dato.

2.3. Elementos clave de la seguridad de la información

Las organizaciones deben ser conscientes de que, aunque tengan un sistema de control, deben implementar prácticas que eviten poner en riesgo la información interna.

Se pueden aplicar ciertas prácticas para garantizar la seguridad de la información, como:

- **Seguridad de aplicaciones:** Se recomiendan procedimientos establecidos en las políticas de la empresa, sobre la protección de las aplicaciones y sus datos.



• **Seguridad en la nube:** Se recomiendan procedimientos establecidos en las políticas de la empresa, para la protección todos los aspectos de la nube, como los sistemas, datos, aplicaciones e infraestructura.

• **Cifrado:** Este control se basa en los algoritmos, ayudando a proteger la información mediante la mezcla de datos, que garantizan que solo los usuarios autorizados puedan leerlos.

- **Recuperación ante desastres:** Se recomienda tener parámetros que ayuden al restablecimiento oportuno del sistema en caso de algún incidente.
- **Respuesta a incidentes:** La organización debe contar con un plan que brinde una respuesta rápida y oportuna para corregir y administrar los datos, ante los eventos disruptivos que puedan afectar la integridad de sus servicios.

- **Seguridad de infraestructura:** Se debe garantizar la seguridad en todos los servicios conectados de la organización, incluyendo software, hardware y redes.
- **Administración de vulnerabilidades:** La organización debe contar con medidas que ayuden en la identificación para la evaluación y corrección de vulnerabilidades que puedan presentarse en su estructura.

Estas prácticas pueden considerarse según el tamaño y sector de la organización. Pero independiente de la cantidad de prácticas que se implementen, están deben estar en constante revisión y Auditoría, para que los controles de seguridad funcionen de forma adecuada. Además, esto ayudara a determinar y se deben actualizar o modificar, ayudando a la mejora continua.

2.4. La seguridad de la información en la organización

Actualmente, la seguridad de la información se ha convertido en un elemento clave para el funcionamiento de las organizaciones, ya que reúne estrategias que ayudan a garantizar la protección e integridad de sus datos, sin que sus actividades se vean afectadas.

Toda organización debe ser capaz de garantizar la resiliencia y sus sistemas de seguridad, con soluciones que no solo aseguren la protección, sino que también permitan conocer el estado actual para prevenir, evitar y solucionar de forma oportuna cualquier tipo de riesgo.



La seguridad de la información conecta tres elementos esenciales para su funcionamiento: las personas, los procesos y la tecnología.



© T-CERT®



Personas

Son cada uno de los miembros de la organización. Desde la gerencia hasta los cargos operativos y de apoyo.



Procesos

Son todos los mecanismos, sistemas y estrategias orientadas a garantizar la seguridad de la información.



Tecnología

Son las herramientas y programas que contribuyen a minimizar los riesgos.



Módulo III. El Sistema de Gestión de Seguridad de la Información – SGSI

Módulo III. El Sistema de Gestión de Seguridad de la Información – SGSI

El Sistema de Gestión de Seguridad de la Información – SGSI, es un conjunto de procedimientos que se utilizan para identificar y mitigar riesgos, garantizando la confidencialidad, integridad y disponibilidad de la información, a través de un proceso de gestión de riesgos, que genera confianza a las partes interesadas.

Se considera importante que el SGSI esté integrado en la gestión general de la organización. Es decir, en sus procesos y estructura. Igualmente, la seguridad de la información debe tenerse en cuenta en el momento de diseñar los procesos, los controles y los medios de información.

El SGSI, debe adaptarse a las necesidades de la organización e incluir toda la información documentada que se defina como necesaria, para la eficiencia de este.

3.1. Ventajas del SGSI

Existen diferentes ventajas en la seguridad de la información cuando se implementa un sistema de gestión, como lo son:



1. Adaptable a las necesidades



2. Establece revisiones correctas para la seguridad de la información



3. Mejora continua



1. Adaptable a las necesidades

1. Adaptable a las necesidades

El SGSI promueve que se establezcan procesos de análisis de riesgos, por lo que se convierte en una herramienta que integra de forma gradual la adopción de criterios que ayudan a mejorar la seguridad de la información, basados en la situación y posibilidades de cada organización.

2. Establece revisiones correctas para la seguridad de la información

Un correcto SGSI, debe iniciar por un análisis que permita evaluar el cómo se verán afectadas las necesidades de la empresa con las amenazas y riesgos de la seguridad de la información. Esto, determinará que se establezcan los controles adecuados para la seguridad de la información, teniendo presente cada actividad, entorno, tamaño y dimensión de cada organización.



2. Establece revisiones correctas para la seguridad de la información

3. Mejora continua



3. Mejora continua

Es importante establecer procesos específicos para garantizar una correcta gestión de seguridad de la información. Estos, ayudaran en el desarrollo de una cultura de seguridad y la gestión del control, garantizando el crecimiento y la mejora continua de la seguridad de la información dentro de la organización.

3.2. Elementos que componen un SGSI

El SGSI está compuesto por varios elementos que se integran para garantizar la protección de los datos. Los más importantes son:



Política de seguridad



Evaluación de riesgos



Plan de seguridad



Controles de seguridad



Auditoria y Monitorización

© T-CERT®



Política de seguridad

- **Política de seguridad:** Generar una política de seguridad de información ayuda a definir los principios y objetivos que gobiernan la protección de los datos. Esta política debe redactarse de forma clara, completa y concisa para el fácil entendimiento de todos los miembros de la organización. Además, debe estar alineada con los objetivos y estrategias de la empresa.



Evaluación de riesgos

- **Evaluación de riesgos:** Este paso, se realiza para identificar y poder evaluar los riesgos a los que se expone la información. Este paso debe ser constante y debe tener presente los riesgos internos y externos.



Plan de seguridad

- **Plan de seguridad:** El plan de seguridad, es un documento que debe incluir las medidas técnicas, organizativas y físicas que se tienen que implementar para la protección de los datos. También debe existir un plan de contingencia para las posibles eventualidades que puedan presentarse.



Controles de seguridad

- **Controles de seguridad:** Se debe contar con medidas concretas que se implementen para proteger la información. Estas medidas pueden ser técnicas (firewalls, antivirus, cifrado, etc.), organizativas (políticas de seguridad, gestión de accesos, etc.) o físicas (control de acceso, cámaras de vigilancia, etc.).



Auditoría y Monitorización

- **Auditoría y monitorización:** La auditoría involucra una revisión metodología del SGSI por un auditor interno o externo, mientras que, la monitorización involucra la supervisión constante de los sistemas y los registros de seguridad. Los dos procesos son usados para la detección de posibles fallos de seguridad o puntos de mejora en el SGSI.

3.3. Quien es el responsable del SGSI

El responsable del SGSI es el equipo de seguridad de la información de la organización. Los miembros de este equipo son responsables de la planificación, implementación, monitorización y mejora continua del SGSI.

Este equipo debe contar con el apoyo y colaboración de todas las áreas de la organización. Ya que, no nos podemos olvidar que es responsabilidad de todos los integrantes de la organización velar por la seguridad de la información.

3.4. Pasos para la creación del SGSI

Para la creación de un SGSI, se deben seguir los siguientes pasos:



© T-CERT®



1. Identificar los activos de información: es imprescindible conocer los activos de información que posee la organización, ya que son la base del SGSI. Los activos de información pueden ser digitales o físicos.



2. Realizar una evaluación de riesgos: Despues de identificar los activos, se deben evaluar los riesgos de seguridad asociados a cada uno de esos activos. Para esto, se debe estudiar el impacto que tendría una pérdida, alteración o divulgación de la información y las probabilidades de que esto pueda suceder.



3. Implementar medidas de seguridad: Se deben implementar medidas de seguridad apropiadas que resguarden los activos de información. Estas medidas pueden ser técnicas, organizativas o físicas.



4. Monitorizar y revisar el SGSI: Es necesario monitorizar y revisar continuamente el sistema, para descubrir posibles fallas de seguridad o áreas de mejora.



5. Mejora continua: por último, es importante manejar una mejora continua del SGSI, que ayude a adaptarse a los cambios del entorno y de la seguridad de la información. Esto se puede lograr implementando estrategias de seguimiento y evaluación.



Módulo IV. Contexto de la organización

Módulo IV. Contexto de la Organización



Contexto de la organización: Detalla las indicaciones para entender a la organización, incluyendo su estructura y objetivos, además plantea la comprensión de las necesidades y expectativas de las partes interesadas. Esto, ayuda a identificar y evaluar los riesgos y oportunidades relevantes para un SGSI dentro de la organización.

Conocer la organización y su contexto, se plantea como un requisito de partida para poder establecer un punto de referencia en la aplicación de un SGSI. El conocimiento de la organización se basa en la definición de todos los factores externos e internos con relación a la seguridad de la información, que pueden ayudar o perjudicar a la consecución del propósito de la empresa.

4.1. Factores externos e internos

La organización debe establecer las cuestiones externas e internas que son relevantes para su propósito y que afecten a su capacidad para lograr los resultados del SGSI.

En la actualidad, las organizaciones deben tener la capacidad de anticiparse y adaptarse a los cambios constantes de la sociedad. Prestar atención al entorno, ayuda a que se pueda estar preparado ante los desafíos y amenazas que puedan presentarse en el camino.

El entorno externo de una organización implica factores políticos, económicos, sociales, tecnológicos, ambientales y legales. Estos elementos ofrecen una comprensión clara de los riesgos y oportunidades que pueden impactar en la organización.

4.1.1. Modelo PESTEL

En el contexto de los factores externos, el análisis PESTEL (o PESTLE) se ha convertido en una herramienta invaluable, que ayuda a las organizaciones a estar preparadas ante los desafíos y amenazas. El análisis PESTEL, es un método representativo usado para conocer el contexto de una empresa.



Factores Políticos: Se deben analizar las políticas del país donde opera la empresa, políticas del sector, la estabilidad estatal y los cambios en los acuerdos internacionales.

Factores Económicos: Los cambios en la normativa fiscal, la inflación, los tipos de cambio e interés, el crecimiento económico, así como la tasa de empleo, son también factores externos que afectan a una empresa.



Económicos



Factores sociales: Se refiere a la valoración de los patrones culturales, valores compartidos, movimientos geográficos de los consumidores y estilo de vida, hábitos y tendencias de consumo.



Factores tecnológicos: Son las inversiones que se realizan para el acceso a la tecnología. Por ejemplo: uso de inteligencia artificial, CRM, entre otros.



Factores ambientales: Son todos los aspectos relacionados con la preservación del medioambiente, desde la contaminación que emite la actividad empresarial y el uso de los recursos naturales, hasta la gestión de los residuos. Para este punto se deben tener presentes las políticas de cada país.



Factores legales: Aquí se deben incluir leyes que puedan afectar y limiten a la organización, como: derechos de autor, licencias, reglas sanitarias, seguridad laboral, salarios, protección del consumidor, etc.

4.1.2. Análisis FODA

El análisis FODA o DOFA, es otra herramienta que sirve para evaluar los factores externos, pero también internos de la organización. Esta puede usarse desde el contexto unipersonal, así como también en grandes proyectos, ya que aporta una visión diferente del cómo se encuentra la organización actualmente.

El análisis FODA está diseñado para comprender la situación de la organización a través del análisis de las fortalezas, oportunidades, debilidades y amenazas.

Analizar las áreas clave en función de las oportunidades y amenazas, ayudará a obtener la información que se necesita para una toma de decisiones estratégica.



Fortalezas



Oportunidades



Debilidades



Amenazas



Fortalezas

Fortalezas: Son las partes de la organización que funcionan bien.



Oportunidades

Oportunidades: Las oportunidades en FODA son el resultado de las fortalezas y las debilidades. Son esas partes que se pueden y se quieren mejorar, y que son aplicables a cualquier actividad de la organización.



Debilidades

Debilidades: Son las actividades internas que no funcionan como debe ser. Al analizar las fortalezas antes que las debilidades, se puede generar una referencia de lo que es exitoso y de lo que no. La identificación de estas debilidades ayuda a generar un punto de partida para mejorar.



Amenazas

Amenazas: Las amenazas son externas, por lo que generalmente están fuera de nuestro control.

Tabla 1. Ejemplo de Matriz FODA

	FORTALEZAS	DEBILIDADES
Factores Internos	<ul style="list-style-type: none"> • ¿Qué es lo que hacemos bien? • ¿Qué hace que seamos especiales? • ¿Qué es lo que le gusta de nosotros a nuestro público objetivo? 	<ul style="list-style-type: none"> • ¿Qué decisiones no funcionan bien y por qué? • ¿Qué podemos mejorar? • ¿Qué recursos o equipos, pueden ayudar al rendimiento?
	OPORTUNIDADES	AMENAZAS
Factores Externos	<ul style="list-style-type: none"> • ¿Qué podemos usar para mejorar nuestras debilidades? • ¿Hay brechas en nuestros servicios? • ¿Cuáles son nuestros objetivos, en X tiempo? 	<ul style="list-style-type: none"> • ¿Qué cambios en el sector son preocupantes? • ¿Hay nuevas tendencias en el mercado? • ¿En qué es mejor la competencia?

Por último, se debe ejecutar una última revisión para confirmar los elementos que determinan la situación actual de la organización.

4.2. Partes interesadas

La organización debe identificar las partes interesadas y los requisitos que son relevantes para el Sistema de Gestión de Seguridad de la Información. Ya que estos pueden influir o pueden ser afectados, cuando de seguridad de la información y la continuidad del negocio se trata.

Principalmente, las partes interesadas podrían incluir:

- Accionistas o propietarios del negocio.
- Empleados y sus familias.
- Entidades gubernamentales y reguladoras.



- Servicios públicos de emergencia.
- Clientes.
- Medios de comunicación.
- Proveedores y socios.
- O cualquier otra persona que se considere importante para el negocio.

Después de identificar las partes interesadas, se deben identificar las necesidades y expectativas que son relevantes para la seguridad de la información. Entre los requisitos de estas, se pueden integrar requisitos legales y reglamentarios, así como obligaciones contractuales, pero todo dependerá de lo que las partes interesadas requieren de la organización y en cómo esta integrará a las mismas en el SGSI.

4.3. Límites y Alcance



La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance. Como primera medida la organización debe identificar cuáles son los activos y procesos de información que respaldan los objetivos y obligaciones.

Se debe realizar un inventario perfecto de los activos y procesos de información, y clasificarlos de acuerdo con su importancia, sensibilidad y criticidad.

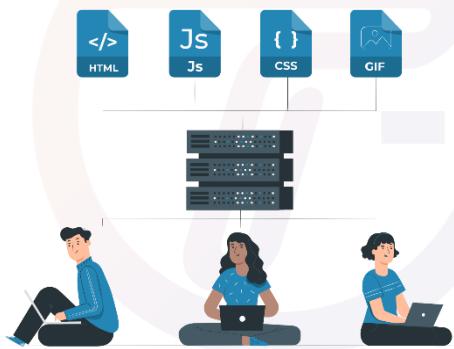
ACTIVOS DE INFORMACIÓN

Son datos, documentos, sistemas o dispositivos que tienen valor para su organización y deben protegerse contra el acceso, uso, divulgación, modificación o destrucción no autorizados.

PROCESOS

Son las actividades y operaciones que implican la creación, almacenamiento, transmisión o procesamiento de activos de información.

Para definir los límites y alcances de un SGSI deben tenerse en cuenta los factores externos e internos, además de los requisitos y objetivos de la seguridad de la información. Al mismo tiempo, se deben considerar las amenazas y vulnerabilidades que puedan afectar los activos y vulneren la seguridad de los datos.



El alcance y los límites del SGSI deben especificar qué partes de la organización están cubiertas o excluidas por el sistema, y qué objetivos y controles de seguridad de la información son aplicables o no aplicables a ellos. El alcance y los límites del SGSI deben estar alineados con todos los objetivos y obligaciones de la organización, por lo que deben ser realistas, alcanzables y medibles.

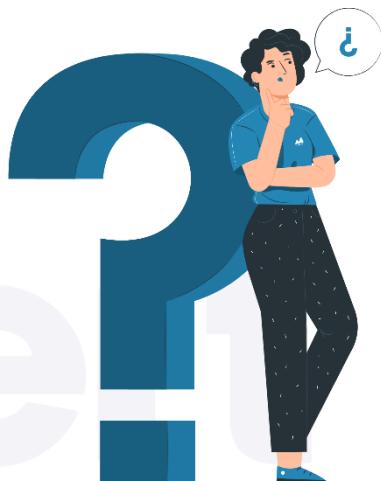
4.3.1. Consideraciones antes de definir el Alcance del SGSI

- Tenga claro los requisitos de seguridad de la información.
- Enumere los servicios críticos que pueden tener un gran impacto en las partes interesadas en caso de fragilidades en la confidencialidad, integridad y disponibilidad.
- Defina el límite y alcance de la organización.

- Defina el límite y alcance de la Tecnología de la Información que posee la organización.
- Defina los límites y el alcance físico.
- Considere las actividades que son externalizadas de cada área.

Estas, son algunas preguntas que pueden hacerse las organizaciones a la hora de definir el alcance y los límites del SGSI:

- ¿Qué productos y servicios estarán cubiertos por el SGSI?
- ¿Cómo y por qué el producto o servicio seleccionado es crítico para la organización?
- ¿Cuáles son las características del servicio seleccionado para ser incluido en el SGSI?
- ¿Requiere que las partes externas cumplan con su SGSI?
- Si las actividades realizadas por la organización requieren de interfaces o dependencias externas o de actividades realizadas por terceros ¿Deberían ser considerados dentro del alcance del SGSI?



Identificar el alcance correcto del SGSI es decisivo, porque ayudará a las organizaciones a cumplir sus requerimientos de seguridad y planificar la implementación del SGSI. Una correcta definición del alcance permitirá:

- Determinar los recursos necesarios. Evadiendo el uso innecesario de recursos (en términos de tiempo, costo y esfuerzo).
- Planificar la implementación del SGSI. Estipulando línea de tiempo y presupuesto.

- Alinear los requisitos de seguridad de la organización, con los objetivos de análisis y evaluación de riesgos.

4.3.2. Cómo definir el alcance de un SGSI

Recordemos que los elementos que debemos tener en cuenta para la definición del alcance son:

1. El contexto de la organización: Las cuestiones Internas y Externas.
2. Los requisitos y expectativas de las partes interesadas.

Cuando se tengan claros estos puntos, los pasos a seguir, son:



1. Identificar lo que necesita ser protegido



1. Identificar lo que necesita ser protegido

Como se mencionó anteriormente, es muy importante que se realice un inventario de activos de información. Con esto determinado, se puede realizar la clasificación de lo que la organización necesita proteger. El análisis y evaluación del riesgo de cada activo determinaran su inclusión en el alcance del SGSI.

El alcance debe definir claramente lo que se está incluyendo, en función de los objetivos y los activos de información que se protegerán, y debe quedar claro que todo lo demás está fuera del alcance.

2. Comprender la organización

Cuando el alcance de un SGSI se define por la necesidad de proteger un activo en específico, es importante entender inicialmente los elementos del sistema y la estructura incluida en la entrega de los servicios. Por ejemplo, el personal comprendido en la administración y entrega de todos los elementos del sistema probablemente será considerado “dentro del alcance”.



2. Comprender la organización

3. Asegurar el apoyo al alcance del SGSI



3. Asegurar el apoyo al alcance del SGSI

El alcance del SGSI debe ser acordado y respaldado formalmente por las partes interesadas más relevantes. Ya que, sin esto, se podrían tener problemas en el momento de implantación del SGSI. Es importante considerar los límites de control y autoridad, especialmente con la seguridad de la información.

4. Monitorear y revisar

El alcance del SGSI no es algo que se realice una vez, este debe estar en revisión constante, además de que puede ser modificado de acuerdo a las circunstancias, las amenazas, las tecnologías o los requisitos. Esto puede establecerse dentro de los objetivos de seguridad, determinando los tiempos de aplicabilidad.



4. Monitorear y revisar

Revise el alcance del SGSI, cuando:

- Aparezcan cambios en el entorno regulatorio.
- Ocurran actualizaciones a estándares o en requisitos de terceros.
- Se haga un cambio en la organización (por ejemplo, cambios en la estructura de la organización).
- Las no conformidades o incidentes indiquen un alcance incorrecto.
- Cambie la madurez general del SGSI (el alcance puede aumentar con el tiempo).
- Exista un cambio en los procesos y las prácticas.
- Surjan cambios en la externalización de servicios

4.3.3. ¿Por qué definir el alcance del SGSI?

- El alcance del SGSI puede reducir el costo inicial en recursos, o potencialmente, aumentarlo.
- La viabilidad y la sensibilidad de limitar el alcance del SGSI dependerá en gran medida de las características específicas de la organización.
- Con un alcance limitado, los activos de la organización fuera del alcance deben tratarse de la misma manera que los proveedores externos a la empresa.



Módulo V. Liderazgo y Compromiso

Módulo V. Liderazgo y Compromiso

Liderazgo y compromiso: Establece los requisitos de liderazgo y compromiso de la alta gerencia para el SGSI. Esto incluye la elaboración y comunicación de la política de seguridad de la información, la asignación de roles y responsabilidades, además del establecimiento de objetivos y planes de mejora continua.



Establecer un plan de seguridad de la información, requiere una participación y compromiso constante de la alta gerencia. Esto, se hace para asegurar que el gobierno de la organización se alinee con la estructura del SGSI. Es importante que el liderazgo de la organización se centre en:



No se puede dejar a un lado que la responsabilidad de la seguridad recae en todos los integrantes de una organización. Aunque, se ha demostrado que el éxito en un plan de seguridad de la información es gracias a un buen liderazgo y compromiso por parte de la alta gerencia.

Proteger la importancia de la seguridad de la información requiere:



- **Compromiso:** Que demuestre los valores éticos y de compromiso con la seguridad en todos los niveles de la organización.
- **Políticas:** Una política y dirección, bien diseñada y estructurada.
- **Enfoque fundado en el riesgo:** Asegurarse de que todos sepan la importancia del enfoque basado en el proceso y el pensamiento basado en el riesgo.

La alta gerencia logra demostrar su compromiso con liderazgo, con respecto al SGSI puede:

- Asegurar que la política y objetivos del SGSI estén establecidos y sean compatibles con la dirección estratégica de la organización.
- Asegurar que los requisitos del SGSI están integrados en los procesos de la organización.
- Garantizar la disponibilidad de los recursos que son necesarios para el SGSI.
- Informar a toda la organización sobre la importancia de la gestión y del cumplimiento de los requisitos del SGSI.
- Asegurar que el SGSI logre los resultados previstos.
- Dirigir y apoyar a las personas para que contribuyan a la eficacia del SGSI.
- Definir roles y responsabilidades correspondientes a la seguridad de la información.
- Garantizar el seguimiento de oportunidades de mejora y éxito de los objetivos de la seguridad de la información, con el objetivo de promover la mejora continua.

5.1. Políticas

POLÍTICAS

Es un documento que expresa una instrucción u orientaciones específicas frente a un área o actividad de una organización, generalmente establecido por la dirección, que debe conocerse y cumplirse.

En la política del SGSI se determinan los objetivos, el marco general, los requerimientos legales y los criterios con los que serán evaluados los riesgos. Es significativo que esta, se redacte de forma en que todos los miembros de la organización puedan entender.

Es importante que la política del SGSI sea aprobada y firmada por la alta gerencia, además de que debe compartirse y comunicarse a todo el personal y partes interesadas, para que estos puedan leerla y entender sus deberes y responsabilidades frente a la información. Recordemos que, todos dentro de la organización son responsables de la seguridad de la información.

Por ejemplo: La clasificación de la información, el control de accesos, uso permitido de activos, la seguridad física y ambiental, el uso de dispositivos móviles, los backups, el manejo de teletrabajo, etc.

La política del SGSI puede apoyarse con políticas específicas, es decir, aspectos más puntuales.

La política debe revisarse, integrarse y actualizarse cuando sea necesario, como en casos donde hay cambios en el entorno, si se detecta un riesgo en la seguridad de la información o si existen cambios organizativos. Es importante que estos procesos se integren en el plan de mejora continua del SGSI.



El desarrollo de políticas específicas ayudará a integrar más fácil los cambios, pues solo requerirá de la actualización en ese documento, sin afectar la política general del SGSI.

5.1.1. Puntos clave en la estructura de la política

- La política debe estar alineada con los propósitos de la organización.
- Incluya objetivos y metas de seguridad de la información, basándose en la triada CIA.
- Considere el alcance del SGSI y su importancia para la organización.
- Incluya el compromiso que tiene la alta gerencia con el SGSI.
- Incluya un compromiso de mejora continua para el SGSI.
- Defina los deberes y responsabilidades de las partes interesadas, frente a la seguridad de la información.
- Defina lo aceptable y lo no aceptable con respecto al uso de los recursos.

Recuerda

La política de seguridad de la información debe:

- Quedar como información documentada.
- Comunicarse dentro de la organización.
- Estar a disposición de las partes interesadas, según proceda.

5.1.2. Pasos para la definición de la política



5.2. Roles y Autoridades

Dentro de toda organización es importante que se definan roles y responsabilidades para cada uno. Esto, hace parte de la gestión organizacional de la empresa, además, ayuda a garantizar que la parte operativa este alineada a los objetivos de la seguridad de la información.

Definir los roles es responsabilidad de la alta gerencia, por lo que esta debe:

1. Asegurarse de que el SGSI se ajuste a los requisitos de la norma ISO/IEC 2001.
2. Asegurarse de estar informada sobre desempeño del SGSI.

Dentro de la seguridad de la información existen diferentes roles y aunque esta sea responsabilidad de todos dentro de la organización, hay uno que sobresale, y este es el propietario de la política y sistema de seguridad de la información.

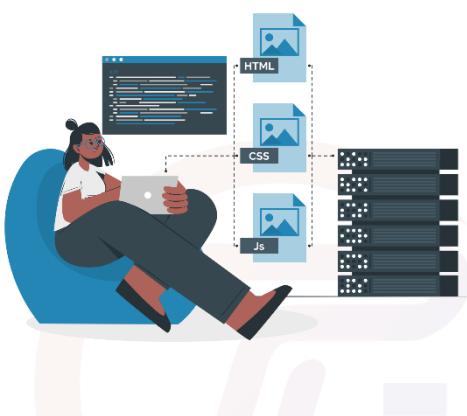
El propietario debe garantizar la implementación de controles y el cumplimiento de la norma. Estos, pueden delegar la implementación diaria de la seguridad en otra persona o proveedor de servicios, pero en última instancia, el propietario es el único responsable. Otros roles característicos en seguridad de la información son:

- **Director de seguridad de la información:** Responsable de todo el personal de seguridad de la información.
- **Especialista en seguridad:** Es el encargado de la protección de equipos de cómputo, infraestructura (software, hardware, redes), datos, y sistemas de información, en caso de algún incidente que ponga en riesgo a cualquiera de estos recursos.
- **Analista de seguridad:** Encargado de analizar y evaluar los incidentes y vulnerabilidades que puedan presentarse en la infraestructura, evalúa las herramientas y procesos de recuperación, además de recomendar soluciones y prácticas de mejora. Puede ayudar en la implementación o administración de seguridad de la información
- **Ingeniero de seguridad:** Es el encargado de monitorizar la seguridad, analizar datos, de registros y generar respuesta a los incidentes que puedan presentarse, debe estar en constante investigación de tecnologías para la mejora e implementación de los procesos de seguridad.
- **Administrador de seguridad:** Es el responsable de instalar y administrar los sistemas de seguridad de la información dentro de la organización.
- **Desarrollador de software de seguridad:** Es la persona encargada de generar software de seguridad, que integren e implementen la seguridad desde el monitoreo, análisis, detección de vulnerabilidades, etc.
- **Criptógrafo:** Es el encargado de proteger la información por medio del cifrado. También puede crear software y ser desarrollador de algoritmos de cifrado más robustos.
- **Analista Criptográfico:** Es el responsable del análisis de la información que se encuentra cifrada, como por ejemplo determinar el propósito de un software malicioso.

- **Usuarios autorizados:** Todas las personas en la organización.

5.2.1. Responsabilidades

Cuando se habla de seguridad de la información, es importante que se asignen responsabilidades sobre las tareas puntuales o específicas, para esto, debe haber una asignación de una persona responsable para cada una de las labores.



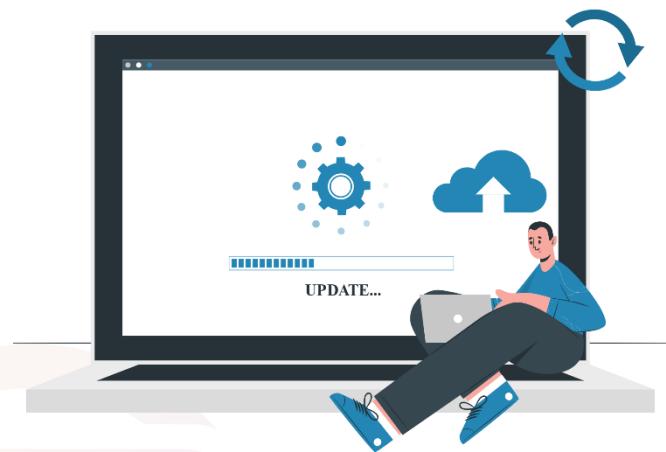
El buen funcionamiento de la seguridad de la información requiere de una verificación de recursos, por lo que se debe hacer un análisis de los recursos que son adecuados para el buen desempeño en las labores asignadas y que, en caso de no tenerlos, asegurarse de que se contrate o capacite al personal, para que puedan desempeñarse de forma idónea.

Este análisis ayudará para que, dentro de los compromisos de la alta gerencia, esté, garantice que se tienen las personas adecuadas para las tareas específicas de seguridad de la información. Garantizando de esta forma que, por ejemplo, cuando se requieran funciones técnicas, la persona encargada y las involucradas, tengan el conocimiento y habilidades necesarias para resolver problemas, utilizar técnicas, métodos, equipos y procedimientos que son relevantes para el funcionamiento del área en la que han sido asignados.

Recuerda

El compromiso de la alta gerencia se confirma con el aporte de los recursos humanos y de materia prima, para garantizar la operación de la seguridad de la información.

Es importante que todo el personal involucrado en la seguridad de la información dentro de la organización se mantenga actualizado frente a los problemas, riesgos, tecnología y prácticas que evolucionan continuamente.





Módulo VI. Planificación

Módulo VI. Planificación



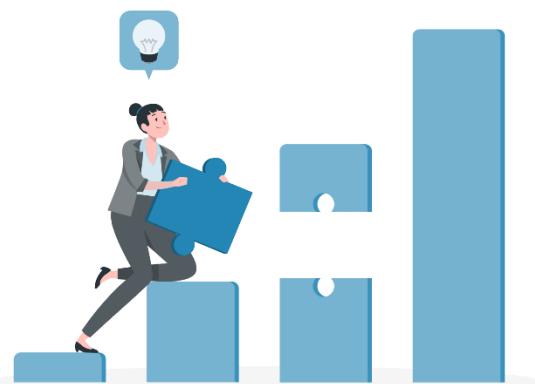
Planificación: Describe los requisitos para planificar el SGSI. La organización debe identificar y evaluar los riesgos y oportunidades. Además, debe definir los objetivos y requisitos de seguridad y la forma en cómo se lograrán. Esto, incluye la selección de controles de seguridad y la elaboración de planes de implementación.

Planificar el SGSI requiere de la identificación y tratamiento de los riesgos y oportunidades. Para lograr esto, es importante considerar los factores internos y externos, los requisitos de las partes interesadas, así como también, los objetivos, límites y alcance del sistema de gestión de seguridad de la información, con el fin de que la organización pueda:

- Garantizar que el SGSI logre los resultados previstos.
- Prevenir o reducir acciones y efectos no deseados.
- Lograr la mejora continua.

Además, la organización debe planificar:

- Las tareas o acciones para abordar los riesgos y las oportunidades.
- Como integrar estas tareas en los procesos del SGSI.
- Como se evaluará la eficiencia de estas acciones.



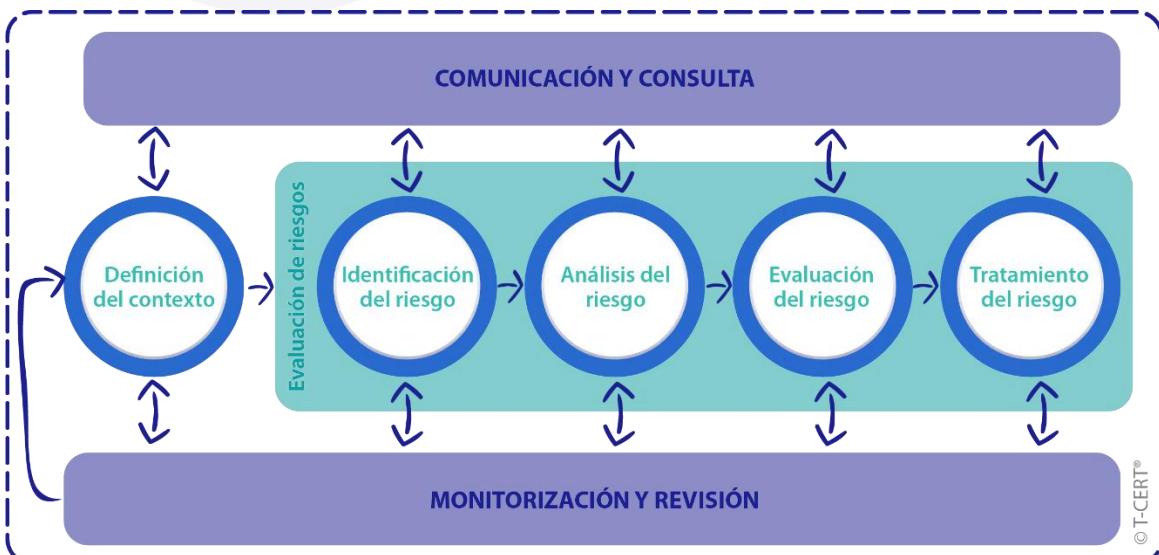
RIESGO

El riesgo indica lo que podría pasar si no se protegen los activos adecuadamente.

La gestión de los riesgos ayuda a implantar conceptos nuevos dentro del análisis de las vulnerabilidades en la seguridad de la información, fortaleciendo la incorporación de acciones que ayudan no solo a abordar los riesgos, sino también a generar oportunidades. Integrar acciones de evaluación y medición ayuda a la mejora continua del SGSI.

El principio para abordar los riesgos y las oportunidades consiste en la evaluación de los riesgos de la seguridad de la información, esta acción nos llevará a proteger la misión y los activos de la organización. Es decir que, se cubrirán las necesidades de la seguridad de la organización, teniendo en cuenta los recursos humanos y económicos, para que la inversión en seguridad sea proporcional al riesgo.

6.1. Ciclo de vida de la gestión de riesgos



El resultado del ciclo de vida de la gestión de riesgos garantiza que se tiene la información necesaria para el tratamiento de los riesgos asociados a la seguridad de la información.

6.2. Identificación de riesgos

El primer paso para la planificación del SGSI es la identificación de riesgos. Por lo que la organización debe definir y aplicar un proceso que ayude a esta evaluación, teniendo en cuenta que:

- Se establezca y se mantengan los criterios de riesgo de seguridad de la información, incluyendo criterios de aceptación y criterios de evaluación.
- Las evaluaciones cuenten con resultados consistentes, válidos y comparables.
- Identifique la implantación y propietarios de los riesgos, esto incluye identificar el riesgo en base a la tirada CIA.
- Se realice un análisis de los riesgos, para posteriormente evaluar las posibles consecuencias en caso de que los riesgos se materializaran. Con esta información, se podrá evaluar la ocurrencia y se asignará un nivel de riesgo.
- Se evalúen los riesgos con el fin de priorizarlos, a través de la comparación con los resultados de análisis y criterios de los riesgos establecidos.
- Se documente el proceso y evaluación de riesgos de la seguridad de la información.



La organización puede contar con la colaboración de diferentes áreas y no solo con el propietario de un servicio en específico, pues no se puede dejar a un lado que la administración de riesgos es la protección de los activos.

6.2.1. Tipos de riesgos

Algunos tipos de riesgos son:

- **Riesgos inherentes:** Son los que se pueden sufrir por el entorno de las operaciones empresariales.
- **Riesgos externos:** son los riesgos que se pueden sufrir por acciones de terceros o eventos externos, de los que no se puede tener ningún tipo de control.
- **Riesgos residuales:** Son los que se pueden sufrir, después de haber aplicado las medidas de control necesarias en la mitigación de riesgos.
- **Riesgos potenciales:** Son los que se pueden sufrir cuando se opera bajo un contexto global, en donde todos los cambios económicos y políticos aumentan los riesgos.

6.2.2. Clasificación de riesgos

Los riesgos se pueden clasificar en una escala por niveles, así:



Lo anterior es una base de lo que puede usar una organización para la gestión de sus riesgos, ya que, cada empresa debe definir los tipos y clasificación de sus propios riesgos. Teniendo en cuenta, como ya se había mencionado, los factores internos y externos, los requisitos de las partes interesadas, su política y objetivos de seguridad de la información.

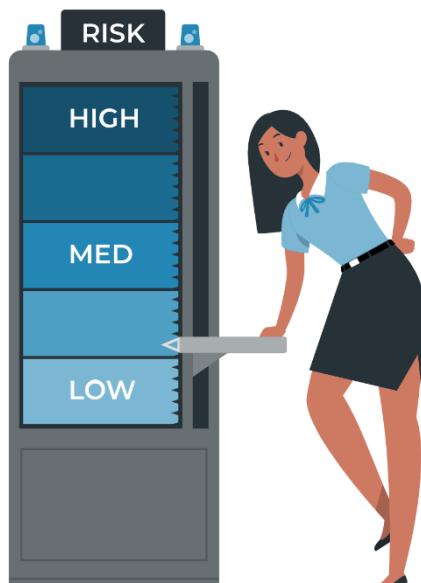
Este proceso consiste en encontrar, reconocer y describir los riesgos de seguridad en la organización. Identificar los riesgos, aporta objetividad a los criterios en los que se apoya la política de la seguridad de la información.

6.3. Tratamiento de riesgos

Después de la identificación de los riesgos de la seguridad de la información, es importante que se implementen acciones para abordar dichos riesgos, en este paso se deben involucrar las partes interesadas, especialmente a la alta gerencia, por la toma de decisiones que se maneja en el tratamiento de los riesgos.

El tratamiento de los riesgos involucra un proceso iterativo de:

- Idear y elegir opciones para el tratamiento de los riesgos.
- Planear e implementar el tratamiento de los riesgos.
- Evaluación de la efectividad del tratamiento de los riesgos.
- Decidir los límites de los riesgos residuales y si sobrepasan estos límites, efectuar un tratamiento adicional.



El tratamiento de riesgos debe comunicarse a las partes interesadas, por lo que se debe considerar el valor y la percepción de este, además de buscar la mejor forma de comunicación, para que la aceptación sea mayor. La organización debe entender que, el tratamiento de riesgos busca la creación y protección del valor.

Es importante que la organización determine los controles necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información elegidas. El anexo A, contiene una lista de controles, sin embargo, la organización puede anexar más si lo considera necesario.

CONTROLES

Son los pasos que se toman para mitigar los riesgos de los datos del negocio y los activos de información.

El proceso de selección de controles, se denomina Declaración de Aplicabilidad, que es donde se define qué tipo de controles son aplicables según los riesgos y amenazas identificados. De esta forma el tratamiento de riesgos tendría como resultado:

6.3.1. El plan de tratamiento de riesgos



La información que debe tener el plan de tratamiento debe responder a:

- ¿Por qué se seleccionaron esas opciones de tratamiento? ¿Qué beneficios se esperan?
- ¿Quién es el responsable de los objetivos?
- ¿Qué acciones se proponen?

- ¿Qué recursos se necesitan? ¿Cuáles son las contingencias?
- ¿Cómo se medirá el desempeño?
- ¿Qué restricciones se tiene?
- ¿Cuál es el plan de seguimiento y revisión? Y Los reportes requeridos.
- ¿Qué plazos se tienen? Incluyendo realización y finalización de actividades.

El plan de tratamiento de riesgos debe ser aprobado por el propietario del activo de información afectado. Toda la información del plan y del resultado, debe estar documentada. Es necesario que se mantenga el plan de seguimiento y revisión, para el control y para que la organización pueda asegurar que la gestión sobre estos es efectiva.

Tabla 2. Plan de seguimiento de tratamiento de riesgos

Código de riesgo	Descripción	Nivel de Riesgo	Proceso de negocio	Activos relacionados	Estrategia	Acciones a Desarrollar	Control de referencia Anexo A	Tipo de Control	Responsable	Plazo

6.3.2. La declaración de aplicabilidad – SOA (Statement of Applicability)

La Declaración de Aplicabilidad – SOA, puede registrarse en cualquier formato, la organización debe definir el que mejor le convenga, ya que en este documento lo más importante es su contenido.

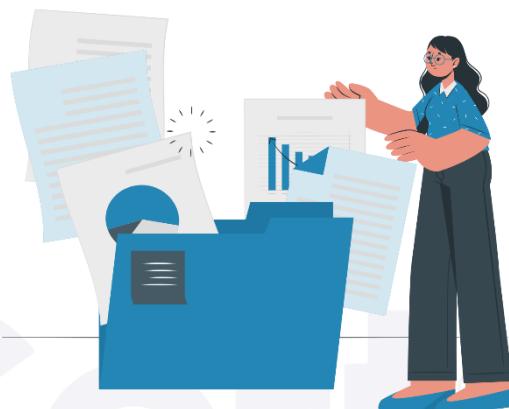
La SOA debe incluir:

- Los controles establecidos.
- Si aplican o no y la justificación de su selección.
- El estado de implementación.
- La documentación relacionada con cada uno (procedimientos, evidencias, etc.).

- Todos los datos adicionales que se consideren necesarios y se deban registrar.

La declaración de aplicabilidad reconoce la trazabilidad de lo que hace la organización, es decir que proporciona una visión amplia de lo que realiza la organización para proteger la información y ayuda en la identificación, organización y registro del plan de seguridad. Además, justifica la inclusión o exclusión de cada control, aspectos que no se incluyen en el informe de Evaluación de Riesgos.

La SOA, debe ser revisada y aprobada por la máxima autoridad de seguridad de la organización, también, debe ser actualizada cuando se deban aplicar nuevos controles o se deban revisar los ya implantados, es decir cuándo:



- Exista nueva información, ya sea interna o externa, también la relacionada con el cumplimiento normativo.
- Se adquieran o sustituyan activos que contengan y gestionen información, que puedan suponer la aparición de amenazas o vulnerabilidades.
- Se realicen cambios organizativos y operacionales que puedan crear cambios en la gestión de la información.
- Se realicen cambios en los requisitos de las partes interesadas.

Es necesario llevar un control de versiones de los documentos SOA que se vayan realizando, registrando todos los cambios realizados.

6.4. Establecer objetivos y requisitos de seguridad

Los objetivos de seguridad de la información deberán:

- Ser coherentes con la política de seguridad de la información de la organización.
- Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y el tratamiento de riesgos.
- Ser objeto de seguimiento.
- Ser informados a las partes interesadas.
- Actualizarse cuando sea necesario.
- Estar disponibles como información documentada.

Cuando la organización planifique como va a alcanzar sus objetivos de seguridad de la información, esta debe determinar:

- Qué se va a hacer.
- Qué recursos se necesitarán.
- Quién será el responsable.
- Cuando se completará.
- Cómo se evaluarán los resultados.

La actualización de cambios en el SGSI, cuando sea necesario, también debe llevarse de forma planificada.





Módulo VII.

Soporte

Módulo VII. Soporte

Soporte: Define los requisitos necesarios para implementar y mantener el SGSI. Para el buen funcionamiento del SGSI la organización debe contar con los recursos, la infraestructura y los recursos financieros. Así como también los requisitos para la competencia, la toma de conciencia y la comunicación e información documentada.



7.1. Recursos

Mantener la gestión de la seguridad durante todo su ciclo de vida requiere cumplir con un mínimo de requisitos, pasando por la planificación hasta la revisión y mejora del sistema. Para esto, la organización debe disponer de:

- **Inversión económica:** La seguridad no es gratuita, por lo que se debe establecer un presupuesto acorde con la evaluación de los riesgos y los criterios de tratamiento.
- **Instalaciones:** La organización debe contar con instalaciones acordes con los niveles de seguridad que implemente, según los riesgos a los que se encuentra expuesta.
- **Equipos:** Mejorar los niveles de seguridad es algo fundamental, por lo que se debe contar con equipos que proporcionen sistemas de defensa o detección de intrusiones en los sistemas de información.
- **Personas:** Recuerda que todas las personas dentro de la organización son responsables de la seguridad de la información, pero no es el objetivo principal dentro de sus labores. Por lo que, la organización puede definir responsabilidades para todos respecto a la seguridad de la información, lo que ayudara a que desempeñen mejor sus funciones y se cumplan los objetivos.



Por otra parte, la organización puede contar con recursos humanos en los que su perfil sea exclusivamente para las tareas del SGSI, estas personas deberán asumir la responsabilidad del cuidado y los objetivos de la seguridad de la información.

7.2. Competencia

La competencia en el SGSI trata de las aptitudes del personal para llevar a cabo las tareas del SGSI, para esto la organización debe:

- Determinar la competencia necesaria de las personas que llevan a cabo el trabajo que afecta el desempeño del SGSI.
- Garantizar que las personas sean competentes sobre la base de su educación, capacitación o experiencia adecuadas.
- Conservar y documentar la información necesaria como evidencia de competencia del personal respecto a la seguridad de la información.

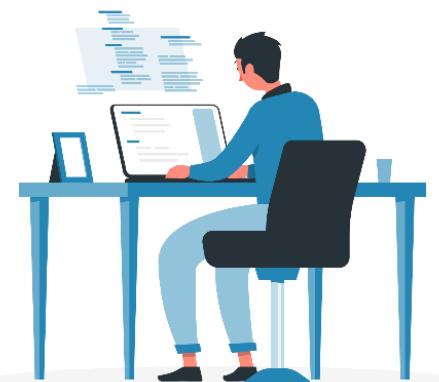
Para garantizar, administrar y realizar el seguimiento de estos requisitos, se puede establecer una matriz de habilidades que contenga los requisitos mínimos, con esto el área de Recursos Humanos puede garantizar una correcta administración y seguimiento de los requisitos.

Esta matriz debe actualizarse cuando sea necesario, ya sea cuando las personas implicadas realicen alguna capacitación o formación, o cuando se requieran nuevos requisitos para garantizar la correcta gestión del SGSI.

Los requisitos que se establezcan para las personas deben aplicar tanto al personal interno como el externo, es decir, cuando la organización requiera de un contratista

externo, este debe contar con las mismas habilidades y cumplimientos de los requisitos establecidos en el SGSI, incluida la documentación de información.

Garantizar las habilidades del personal, implica que estos comprendan lo que significan para la organización y como contribuyen para el cumplimiento de los requisitos de seguridad de la información. Por esta razón, la organización debe contar con una gestión de comunicación y un proceso de capacitación donde:



- Se proporcione capacitación o se tomen medidas para asegurar que las personas cuenten con las habilidades necesarias para el cumplimiento de competencia dentro del SGSI.
- Se monitorean constantemente los niveles de competencia, para definir posibles brechas.
- Planificar lo que se haría, es decir, el paso a seguir en caso de encontrar brechas.

Es importante que cuando se ejecute un proceso de capacitación, se integre dentro de este, un formato de evaluación, que ayude a determinar que las habilidades de cada persona han mejorado y que así mismo se vea reflejado en el desempeño de sus tareas. Esto también hace parte de determinar la competencia del personal, con respecto al SGSI.

La norma no exige un aprendizaje de memoria de la política de seguridad de la información, pero si **necesita que las personas comprendan sus responsabilidades** y como se ajusta su función dentro de la organización.

7.3. Conciencia

Las personas que hacen parte de la organización y que se encargan del funcionamiento del SGSI, deben ser conscientes de:

- La política de seguridad de la información.
- Su contribución a la eficacia del SGSI, así como también los beneficios de la mejora del rendimiento de la seguridad de la información
- Las implicaciones de una no conformidad frente a los requisitos del sistema de gestión de la seguridad de la información.

7.4. Comunicación



Dentro de la organización existe comunicación interna y externa, ambas son relevantes para el SGSI, por lo que se debe establecer una necesidad en las comunicaciones que se realicen, en donde se indique:

- Lo que se debe comunicar.
- Cuando se debe hacer una comunicación.
- A quien dirigir la comunicación.
- Como se debe comunicar.

7.5. Información documentada

Cuando se cree o se actualice información documentada, la organización debe garantizar:

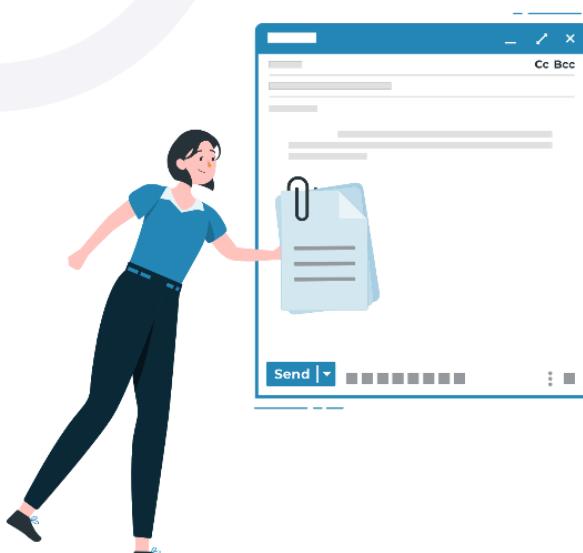
- La identificación y descripción: Como título, área, informe, etc.
- El formato y soporte: Como el idioma, la versión de software, si es impreso o electrónico, etc.

- La revisión y aprobación de la disposición y adecuación.

La información documentada que requiere el SGSI debe ser controlada, garantizando que:

- Se encuentre disponible y es adecuada para su uso, donde y cuando se necesite.
- Se encuentre protegida.
- Se tenga un control, que responda a:
 - ✓ La distribución, acceso, recuperación y uso.
 - ✓ El almacenamiento y conservación.
 - ✓ Control de cambios.
 - ✓ Conservación y eliminación.

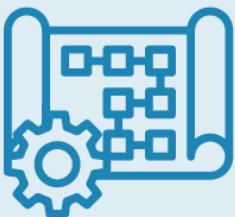
La información documentada que es de origen externo, clasificada por la organización como necesaria para la planificación y operación del SGSI, se debe identificar como apropiada y controlada.





Módulo VIII. Operación

Módulo VIII. Operación



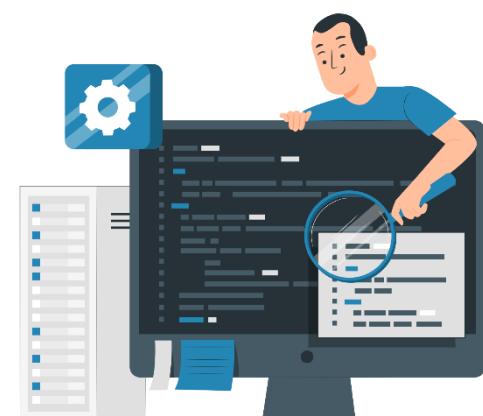
Operación: Indica los requerimientos para la planificación, la implementación y el control de los procesos de la organización. Se incluyen requisitos para la gestión de riesgos, la seguridad de la información, la documentación y el control de seguridad y accesos.

8.1. Planificación y control

La organización debe contar con requisitos para controlar que se toman las medidas adecuadas para conseguir los objetivos de seguridad de la información, y la mejor forma de demostrar que se cumplen estos requisitos es por medio de los registros, es decir que se debe contar con la evidencia para cada control que se haya establecido.

8.1.1. Control de cambios

Para este punto se debe idear una forma de cómo manejar los cambios programados y los que no han sido programados que puedan afectar la seguridad de la información. Es importante identificar, los efectos que los cambios tienen en los sistemas y que acciones se implementaron para disminuir su impacto.



Es decir que, se debe gestionar cualquier evento dentro de la seguridad de la información, para esto se debe registrar o documentar:

- Todo el proceso respecto a los cambios controlados.

- Los incidentes en la seguridad de la información.
- Las Auditorías y sus resultados.
- Las reuniones de revisión de los sistemas de información y objetivos del SGSI.

Toda la información sobre los eventos de la seguridad de la información debe estar al día, los datos recopilados permitirán que se puedan revisar en cualquier momento para un respectivo análisis, en donde se podrá identificar de forma ágil y rápida lo que no funciona y se podrán realizar los cambios necesarios para que estén acorde a los requisitos del SGSI.

Recuerda

Realizar copias de seguridad de la información documentada de la organización.

8.2. Evaluación de riesgos

Se deben implementar evaluaciones de los riesgos, este proceso ya debe estar definido, por lo que también es importante que se defina cada cuánto se realizaran, que puede ser de forma regular o cuando sea necesario.

Los pasos para la evaluación del riesgo de la seguridad de la información son:



8.2.1. Identificar los activos de información

1

Identificar los activos de información

Los activos se pueden identificar en dos grandes grupos: tangibles e intangibles. Los activos tangibles son aquellos activos materiales que contienen información, y sobre los que se toman medidas preventivas para su protección principalmente de riesgos físicos: golpes, agua, fuego, etc.

Los activos intangibles son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno.

Cada activo debe contar con una “propiedad de los activos”, esta debe incluir:



© T-CERT®

8.2.2. Clasificar la información

La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. El sistema de clasificación se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la confidencialidad, la integridad y la disponibilidad de cada activo.

2

Clasificar la información

Para realizar una correcta clasificación de activos según la confidencialidad, integridad y disponibilidad se recomienda la utilización de las siguientes tablas:

Tabla 3. Clasificación de acuerdo con la confidencialidad

Confidencial	Acceso restringido a la alta dirección
Restringido	Directores de área y empleados clave tienen acceso.
Interno	Relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel.
Público	Todas las personas dentro y fuera de la organización, tienen acceso.

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejen en cada organización.

Tabla 4. Clasificación de acuerdo con la Integridad

A (Alta)	Información cuya perdida puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o generar perdidas de imagen severas de la organización.
M (Media)	Información cuya perdida puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o generar perdida de imagen moderado a funcionarios de la organización.
B (Baja)	Información cuya perdida no genera un impacto significativo para la organización o entes externos.
No clasificado	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

La integridad se refiere a la exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

Tabla 5. Clasificación de acuerdo con la disponibilidad

1 (Alta)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o generar perdidas de imagen severas a entes externos.
2 (Media)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o generar perdida de imagen moderado de la organización.
3 (Baja)	La no disponibilidad de la información puede afectar la operación normal de la entidad, entes externos, pero no conlleva implicaciones legales, económicas o de perdida de imagen.
No clasificado	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

8.2.3. Evaluar la información



Se debería desarrollar e implementar un conjunto adecuado de procedimientos para la evaluación de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

A continuación, se proponen una serie de ítems que podrían ser tenidos en cuenta para realizar este proceso y se deberían tener en cuenta las siguientes pautas generales:

- Etiquete todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.
- Etiquete el nivel de clasificación con relación a la confidencialidad, la integridad y la disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente, se debe diligenciar la clasificación de la siguiente forma: {Clasif.Confidencialidad} - {Clasif.Integridad} - {Clasif.Disponibilidad}.
- Para los activos clasificados en confidencialidad se podría utilizar la etiqueta IC, IR, IP, ISC.
- Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.
- Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.



8.2.4. Definir los controles

Defina los controles que requiere de acuerdo con la lista del anexo A, sin embargo, recuerde que la organización puede anexar más si lo considera necesario.



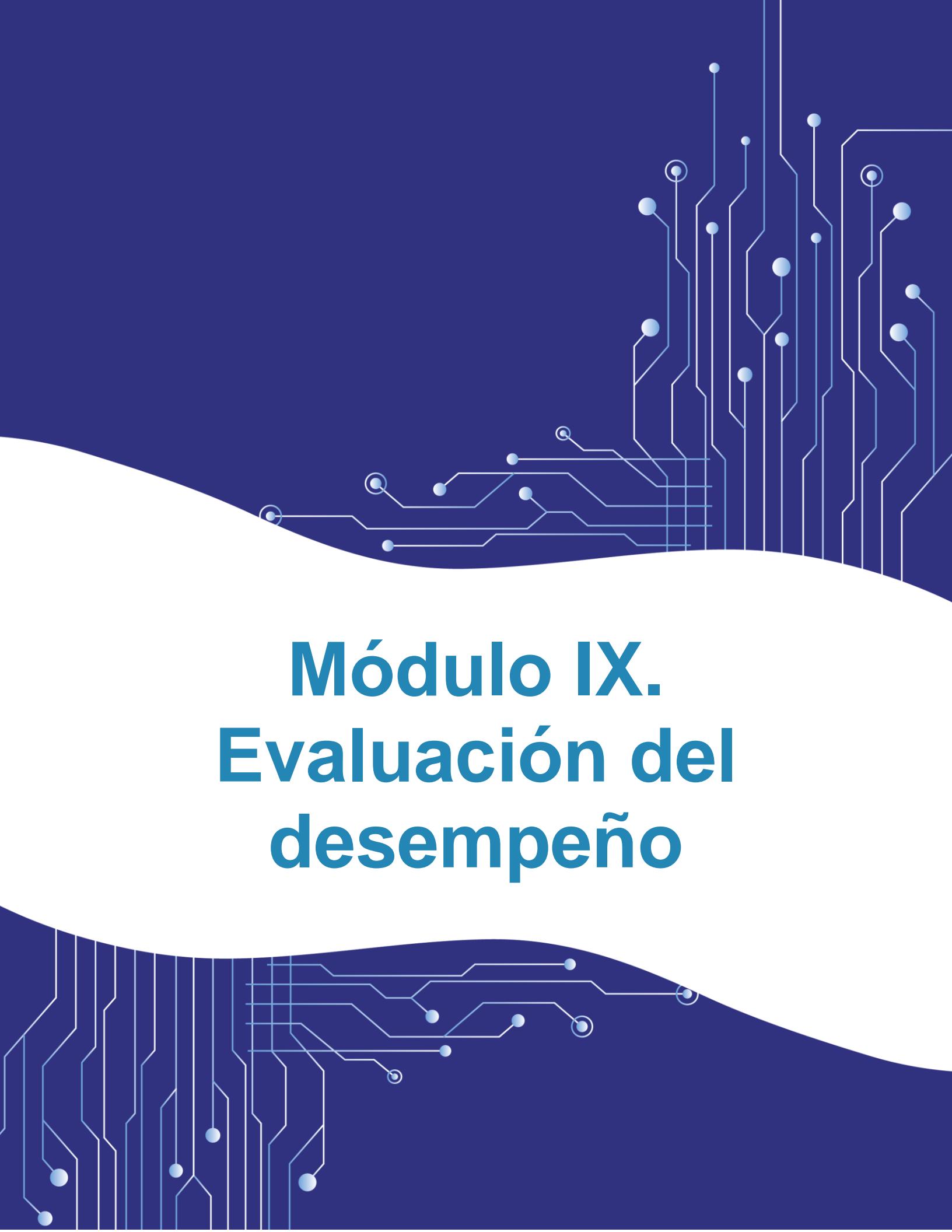
8.3. Tratamiento de riesgos

Después del análisis y evaluación de los riesgos de seguridad, debe realizarse un plan de tratamiento de riesgos, esto garantiza que se implementen los controles correctos para mitigar el riesgo en la seguridad de la información. El tratamiento de riesgos es el resultado de la evaluación del riesgo y de la declaración de aplicabilidad – SOA.

El plan de tratamiento de riesgos es un documento que:

- Recoge la descripción de las actividades que se realizan.
- Determina los responsables de las actividades.
- Registra la trazabilidad entre las medidas y los riesgos.

Es importante que las métricas estén alineadas con los objetivos de la organización, que se han definido previamente.



Módulo IX. Evaluación del desempeño

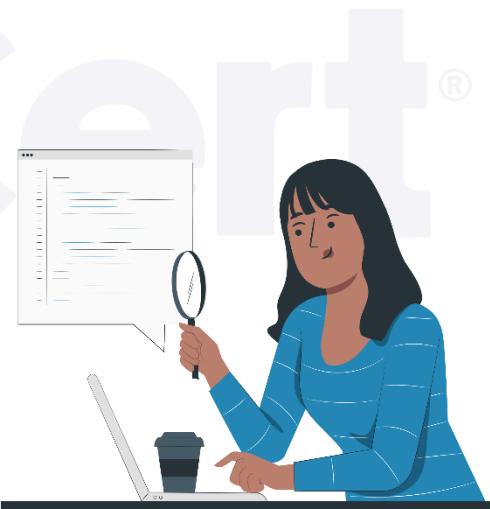
Módulo IX. Evaluación del desempeño

Evaluación del desempeño: Establece los requisitos para llevar a cabo la medición, el seguimiento, el análisis, la evaluación, la realización de auditorías internas y las revisiones de gestión y evaluaciones del desempeño del SGSI.



La organización debe llevar a cabo una evaluación de rendimiento de la seguridad de la información y de la eficiencia del SGSI, además de establecer un programa de auditoría. Esto, porque es importante que la organización pueda demostrar que si está tomando medidas para lograr los objetivos y la mejor forma de hacerlo es por medio de registros.

La eficacia del SGSI se puede medir con auditorías internas, estas deben incluir la frecuencia, los métodos, las responsabilidades, requisitos de planificación y los respectivos informes. Este proceso ayudara a saber si se está cumpliendo con la norma y también con los requisitos específicos de seguridad de la información que haya establecido la organización.



Como se mencionó antes, la organización debe establecer un programa de auditoría, esto, porque se considera la herramienta más efectiva a la hora de medir el SGSI, cuando se realice este proceso se debe considerar la importancia de los procesos y el resultado de auditorías anteriores.

9.1. Monitoreo, medición, análisis y evaluación

El primer paso para medir el rendimiento del SGSI es conocer y establecer de que información se requiere evaluar el cuándo, quien y como.

9.1.1. Optimizar los recursos

Evalué solo lo realmente necesario, es decir, solo supervisé y evalúe los recursos que cumplan con el requisito de evaluar la seguridad de la información y la eficiencia del SGSI.

9.1.2. Establecer metas

Defina las metas de su organización de acuerdo con el punto donde se encuentre la ejecución del SGSI, estas metas se definirán según el nivel de conciencia sobre la seguridad de la información que se perciba en la organización, además deben revisarse en periodos determinados y cambiarse según corresponda.

9.1.3. Medir la efectividad del SGSI



Un SGSI que está siendo correctamente implantado es la clave para que la organización pueda alinear los procesos de TI con los procesos operativos y comerciales. Integrar la seguridad de la información en los procesos ayudará a reducir los niveles de riesgo.

Un SGSI efectivo tiene beneficios como:

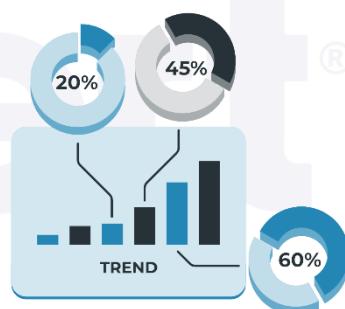
- Demostrar el valor de la seguridad de la información, los procesos de seguridad de TI y los controles adaptados.

- Controles efectivos y comprendidos dentro del valor.
- Integración de procesos de gestión de riesgos de la seguridad de la información con los procesos de gestión de riesgos empresariales.
- Toma de mejores decisiones estratégicas.
- Creación de confiabilidad entre las partes interesadas y externas.
- Facilidad de adaptación a los cambios.

Es importante que la organización establezca la medición como uno de los requisitos clave de SGSI, ya que esto ayudará a su operación. La decisión sobre qué medir, los factores críticos de éxito o los objetivos de medición deben ser definidos por la organización y deben ser parte de la alineación del SGSI con las estrategias y los objetivos del negocio.

MÉTRICA

Son los valores expresados numéricamente que sirven para analizar el rendimiento de una determinada acción o proceso dentro de una empresa. Cualquier cosa que se realice dentro del ámbito empresarial y sea medible, es una métrica.



Algunos ejemplos de mediciones pueden ser la escala de porcentaje de disponibilidad, porcentajes, números, fracasos/éxito, escalas de madurez, como la escala de madurez de CMMI o COBIT e incluso una escala de nivel de satisfacción, todas son consideradas métricas.

Medir la efectividad de los procesos del SGSI, es medir su desempeño frente a los objetivos predefinidos, desviaciones de los objetivos o nivel de satisfacción, después la organización puede agregar el factor del tiempo, asegurando la comparabilidad y la detección de cambios con el tiempo.

Los cinco procesos más importantes del SGSI, son:



9.2. Auditoría

AUDITORÍA

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

9.2.1. Tipos de Auditoría

Tabla 6. Tipos de Auditoría

Auditorías de primera parte (Auditorías internas)	Auditorías de segunda parte	Auditorías de tercera parte (Auditoría externa)
Son las realizadas por la misma organización con su personal o una parte externa en su nombre, es decir, una empresa subcontratada.	Son las realizadas por partes que tienen interés en la organización o por personas en su nombre, habitualmente se realizan a un proveedor que se requiera para algún suministro y se necesite comprobar su nivel de cumplimiento con los requisitos establecidos.	Se trata de una auditoría en la que una entidad de certificación acreditada comprueba el cumplimiento de los requisitos de la norma, así como su implementación y mejora.

9.2.2. Auditoría interna

Dentro de los requisitos del SGSI se incluye la realización de auditorías internas a intervalos planificados, que incluyen uno o más programas de auditoría, selección de auditores y objetividad e imparcialidad del proceso de auditoría.



La auditoría interna es un aspecto clave dentro del SGSI, sus objetivos principales son la planificación y la independencia de los auditores. Además, proporciona información sobre si el SGSI cumple con los requisitos propios de la organización para su SGSI, así como con los requisitos de la norma.

Para organizaciones pequeñas este paso de independencia suele ser difícil, por la disposición que requiere de los recursos para implementar y mantener, además del requisito de recursos capacitados e independientes para realizar las auditorías internas.

Un programa de Auditoría debe contemplar:

- La frecuencia y las fechas previstas.
- El alcance de la auditoría interna.
- Los métodos por los cuales se llevará a cabo la auditoría interna.
- La asignación de responsabilidades para la planificación, la realización y la presentación de informes de los resultados de la auditoría interna.

9.2.2.1. Criterios de Auditoría

CRITERIOS DE AUDITORÍA

Referencias que se utilizan para comparar las evidencias de la Auditoría. Se trata de definir lo que se va a auditar.

Cada auditoría planificada debe generar información documentada como evidencia de la implementación del programa y los resultados de la auditoría. En esta información se debe incluir la documentación de los criterios y el alcance de la auditoría, para garantizar que se cumplen los objetivos.

9.2.2.2. Requisitos de la auditoría

Los requisitos se refieren a las referencias de aprobación para la Auditoría, por ejemplo, el cumplimiento de:



Los requisitos
ISO 27001

© T-CERT®



Los requisitos
legales



El proceso de
organización / Políticas /
Procedimientos, etc



Los requisitos del
cliente o partes
interesadas

9.2.2.3. El alcance de la auditoría

El alcance de la auditoría incluye una descripción de la ubicación física, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto. Es decir, que reconoce:

- El tiempo en que se realizará la auditoría (inicio y fin).
- Qué y a quién se va a auditar.

- Donde se realizará la Auditoría.

9.2.2.4. Selección de los auditores

Es necesario seleccionar un equipo de auditoría, en donde lo más importante sea su independencia e imparcialidad. La independencia de los auditores consiste en que los responsables de llevar a cabo la auditoría no puedan auditar funciones o procesos sobre los que tienen control o propiedad operativa.

9.2.2.5. Informar los resultados

El auditor interno tiene la responsabilidad de garantizar que los resultados se informan a la alta gerencia de la organización.

Los resultados del plan de auditoría y los registros recopilados durante las actividades, deben guardarse como información documentada, tanto del plan de Auditoría como del registro del desempeño del SGSI, garantizando el cumplimiento de los objetivos.



9.3. El auditor interno

Un auditor interno:

- **Planifica su Auditoría:** es responsable de identificar qué proceso le toca auditar, investiga sobre el mismo, identifica riesgos y oportunidades y también identifica la información documentada necesaria para evidenciar el cumplimiento a los requerimientos.

- **Realiza la auditoría:** Realiza la auditoría, identificando las evidencias necesarias para demostrar cumplimiento o incumplimiento a los criterios definidos en el plan de seguridad de la información.
- **Identifica los hallazgos:** Dentro de la realización de la Auditoría, una vez que identifica las evidencias que demuestran cumplimiento o incumplimiento de los requisitos, identifica si existen hallazgos y se los hace saber al dueño del proceso auditado.
- **Realiza el reporte de Auditoría:** Describe los hallazgos encontrados, anexando la evidencia objetiva que lo demuestre y junto con el auditor líder califica los hallazgos.
- **Adquiere nuevas competencias:** La última de las responsabilidades del auditor interno es ser partícipe de los procesos de desarrollo que se han identificado para mejorar su competencia.



El rol de auditor interno ayuda a una organización a cumplir sus objetivos, aportando un enfoque sistemático y disciplinado, para evaluar y mejorar la eficiencia de los procesos de gestión de riesgos.

El auditor interno representa en una organización el principal apoyo de las partes interesadas para la administración y monitoreo continuo de los riesgos que puedan impedir el cumplimiento de los objetivos de negocio.

La función de auditoría interna vigila el cumplimiento de los controles internos diseñados por la gerencia y agrega valor a la organización, proporcionando

recomendaciones para corregir las debilidades de control interno y para mejorar la eficacia de los procesos.

El auditor interno se asegura principalmente de que:

- Los riesgos estén identificados y gestionados de manera apropiada.
- Los asuntos significativos en materia legal o regulatoria que impactan a la organización son reconocidos y direccionados apropiadamente.
- La información significativa sobre aspectos financieros, administrativos y operativos es exacta, confiable y oportuna.
- Los empleados actúan conforme a las políticas, procedimientos y regulaciones.
- Los recursos adquiridos son utilizados y protegidos eficientemente.
- Los programas, planes y objetivos son alcanzados.
- La calidad y mejora continua forman parte integral de los controles.

9.4. Revisión por la dirección

La norma establece que la alta gerencia debe realizar una revisión o examen periódico del SGSI, en donde junto con las partes interesadas se revise el desempeño y se mida la efectividad del SGSI, convienen realizarse a intervalos regulares para revisar el progreso y las acciones requeridas para mejorar el sistema.



Los tiempos de revisión pueden cambiar de acuerdo con las necesidades del SGSI, por ejemplo, en un periodo inicial las reuniones pueden ser mensuales y después pueden programarse de forma trimestral o semestral.

Quien debería asistir a las revisiones:

- Gerentes operativos.
- Gerentes de recursos humanos.
- Directores de TI.
- Gerentes de seguridad de la información.
- Gerentes de calidad.
- Propietarios de activos o riesgos.
- Cualquier persona dentro de la organización que tenga acciones o responsabilidad del SGSI.



Las partes interesadas solo deben ser tenidas en cuenta a nivel de gestión y consultadas cuando sea necesario.

Las personas que acuden a las reuniones para la revisión pueden cambiar de una reunión a otra, esto dependerá de los riesgos que se hayan identificado, los activos y acciones que se vayan a revisar.

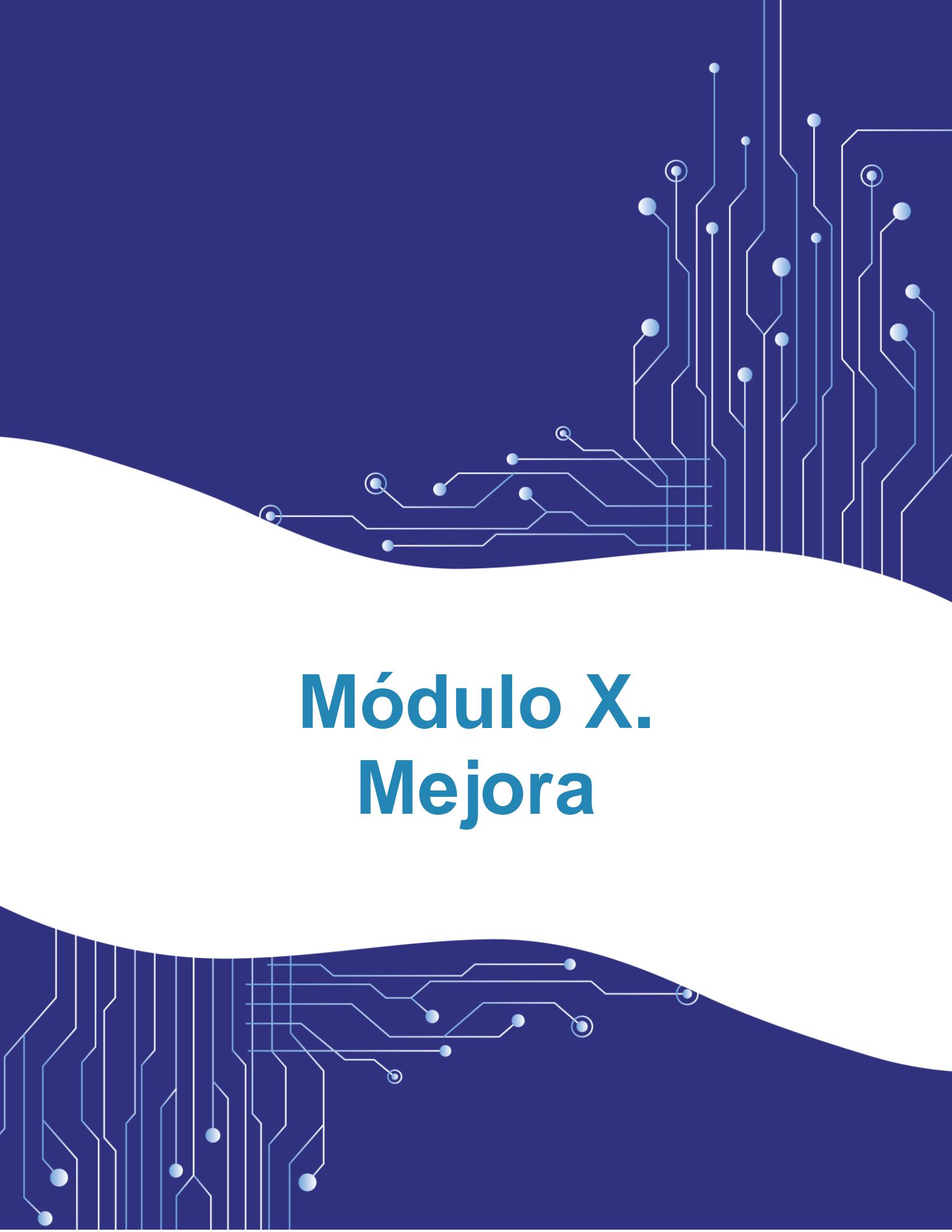
Restrinja en lo posible las reuniones sobre la revisión del SGSI solo a las partes interesadas, es decir, no incluya a la alta gerencia que no esté interesada en los aspectos operativos del sistema.

La revisión por la dirección puede incluir:

- Introducción:
 - Propósito de la reunión.
 - Comprobar la lista de asistentes.

- Revisión de las Revisiones anteriores:
 - Revisar informes de reuniones anteriores.
 - Verificar el estado de las acciones.
 - Registrar el estado de acciones completadas vs acciones en curso.
 - Cerrar las acciones que han sido completadas.
- Revisión de cuestiones internas y externas.
- Revisión del alcance y los objetivos del SGSI.
- Revisión del desempeño y la mejora continua del SGSI:
 - no conformidades y acciones correctivas.
 - resultados del seguimiento y medición.
 - resultados de auditoría.
 - cumplimiento de los objetivos de seguridad de la información.
- Revisión de los recursos, presupuestos y otros temas relacionados con las limitaciones del SGSI.
- Revisión de la evaluación de riesgos.
- Revisión de las políticas y procedimientos de seguridad de la información.
- Métricas de rendimiento / KPI:
 - Métricas de rendimiento y los KPI.
 - Análisis de los resultados de incidentes recientes y análisis causal.
- Cierre de la reunión
 - Confirmar acciones y propietarios de acciones.
 - Confirmar planificación de tiempo para acciones.
 - Confirmar fecha y hora de la próxima reunión.

Sin importar el enfoque que se adopte para las revisiones de la dirección, se debe confirmar que todos los niveles de dirección fueron involucrados y están al tanto del SGSI y su propósito.



Módulo X. Mejora

Módulo X. Mejora



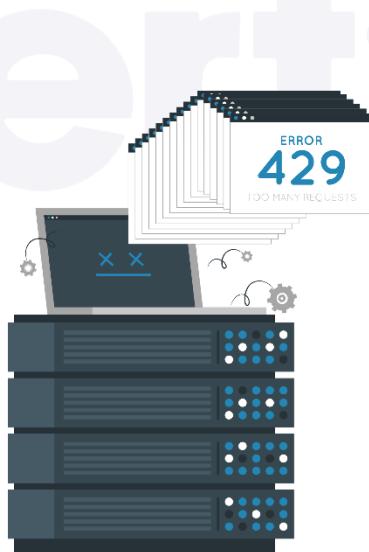
Mejora: La organización tiene la responsabilidad de generar una cultura que se centre en la importancia de mejorar continuamente para la adecuación y eficacia del SGSI.

La mejora puede y debe aplicarse en todas las áreas y niveles de la organización, todos los implicados y partes interesadas deben tener presente la mejora continua para maximizar la eficacia de los servicios.

Es importante reconocer que por más que se establezcan acciones para afrontar los riesgos, es inevitable que se produzcan incidentes debido a las no conformidades, tanto reales como potenciales.

10.1. No conformidad, acción correctiva

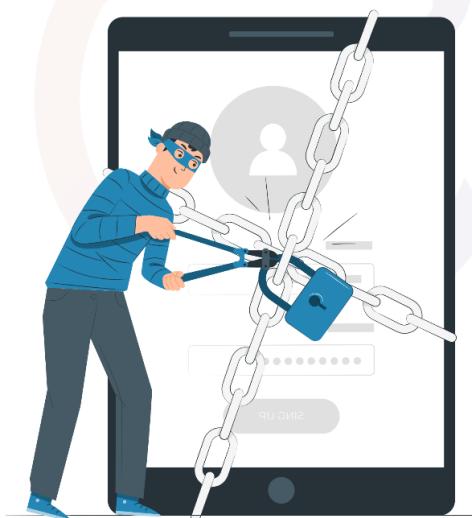
Las no conformidades, se identifican habitualmente como incumplimientos normativos o sobre procesos internos propios de la organización. Identificarlos garantiza que las acciones correctivas empleadas son adecuadas para la mejora continua del sistema.



La organización debe definir qué es una no conformidad, algunos tipos de no conformidades que se pueden identificar en un SGSI, son:

- Incumplimiento con un requisito o control establecido en el SGSI o simplemente que está mal implementado.

- Incumplimiento total o parcial de los requisitos legales, contractuales o acordados del cliente.
- Incumplimiento detectado en comportamientos que violan los procedimientos y políticas establecidos para la seguridad de la información o políticas de la empresa.
- Desvíos en los productos o servicios acordados con proveedores en cuanto a los requisitos para la seguridad de la información.
- Proyectos que entregan resultados fuera de los parámetros esperados.
- Controles para la seguridad de la información que no cumplen con lo planificado, no se han aplicado correctamente o han demostrado ser ineficaces.
- Actividades previstas dentro del SGSI que no se realizan con la eficiencia esperada.



- Incidentes para la seguridad de la información producidos por incumplimientos de requisitos del SGSI.
- No conformidades por denuncias de los clientes.
- Alertas denunciadas por usuarios, proveedores u otras partes interesadas.
- Resultados de sistemas de monitoreo que revelan incumplimientos en los criterios de aceptación.
- Objetivos no alcanzados.

Es esencial que la organización priorice y aplique acciones correctivas para los problemas más importantes y los que se deban resolver de forma urgente. Después, debe abordar las no conformidades que no son tan importantes, pero que ayudan a mejorar la eficiencia del SGSI.

10.1.1. Plan para la mejora

Siga los siguientes pasos para ayudar a la mejora en su organización:



10.1.1.1. Paso 1: Registre todo lo que sea posible

Defina los objetivos para conservar la información y el registro de cosas.

Por ejemplo:

- Alertas de malware.
- Tentativas de intrusión.
- Vulnerabilidades de correo electrónico.
- Usos inadecuados de dispositivos (Bring Your Own Device – BYOD, Accesos a internet, etc.).
- Detecciones de denegación de servicios o accesos.



10.1.1.2. Paso 2: Investigar y comunicarse

Investigar y comunicarse

PASO
2

Investigue y manténgase al tanto de las amenazas que aparecen en las actividades realizadas, también, comuníquese con entidades de ciberseguridad para intercambiar información relevante. De esta forma puede establecer registros para nuevas amenazas e implementar acciones correctivas para las no conformidades detectadas.

10.1.1.3. Paso 3: Aborde las no conformidades

La organización debe diferenciar las acciones inmediatas y las que se abordan en un plan con objetivos para la eliminación de las no conformidades. Por lo que debe:

1. Identificar el alcance y el impacto de la no conformidad.
2. Establecer acciones correctivas para limitar el impacto de la no conformidad, las correcciones no deben empeorar la situación, para esto:
 - Maneje una buena comunicación de las acciones correctivas, asegurándose que se realicen las correcciones.
 - Implemente las correcciones.
 - Supervise y cerciórese de que las correcciones tengan el efecto esperado y no hayan producido efectos secundarios no deseados.
 - Tome acciones para corregir la no conformidad, si aún no se ha remediado.
 - Comuníquese con otras partes interesadas relevantes.

3
PASO

Aborde las no conformidades

Las acciones correctivas se pueden abordar con los siguientes criterios:

- **Decisiones para llevar a cabo una acción correctiva:** Establezca un proceso de toma de decisiones sobre las acciones correctivas.

- **Revisión de la no conformidad:** Analice los comportamientos y apóyese en el uso de algoritmos, para saber si se han registrado conformidades similares.
- **Análisis de las causas de la no conformidad:** Analice las causas, para poder determinar las acciones adecuadas y eficaces para evitar que la no conformidad se vuelva a producir. Apóyese en métodos sistemáticos que le ayuden a identificar:
 1. Los desvíos básicos: Evidencias de error o fallos.
 2. Los indicios: los incidentes adversos identificados y los pasados por alto.
 3. Los problemas superficiales causados.
 4. Los problemas que cuando se trataron, se eliminó también su causa para que no se volvieran a producir efectos no deseados.
- **Análisis de posibles consecuencias sobre el SGSI:** Evalué la necesidad de realizar modificaciones en el SGSI.
- **Establezca acciones para corregir la causa:** Identifique el problema y tome las acciones necesarias para eliminar o evitar impactos más graves en la seguridad de la información.
- **Implemente acciones correctivas:** En lo posible, de prioridad a las áreas donde hay mayor probabilidad de recurrencia y las consecuencias más significativas de la no conformidad.
- **Evalúe las acciones correctivas:** Determine si realmente se han gestionado las causas de la no conformidad y si se ha evitado que ocurran las no conformidades relacionadas.

Documento las evidencias

10.1.1.4. Paso 4: Documente las evidencias

**PASO
4**

Como se ha mencionado antes, es importante que documente y se guarden los registros de la identificación de las no conformidades y las acciones que se han tomado para borrarlas, así como de sus resultados.

10.2. Mejora continua

MEJORA CONTINUA

Práctica de gestión enfocada en la mejora constante de procesos operativos, con el objetivo de ser más eficiente y tener un mejor rendimiento.

Se habla de que la mejora continua se basa en tres pilares principales, los cuales son:



1

Continuidad: siempre hay una forma de mejorar y esta búsqueda debe ser constante, ya que no existe la perfección en los procesos.

2

Cultura: es importante que dentro de la organización se forme una cultura de mejora, para que la continuidad sea posible, es necesario volver esa cultura en un hábito.

3

Bueno para todos: las mejoras deben estar pensadas y deben ejecutarse para que contribuyan beneficios a todas las áreas de la organización. Involucre a todas las partes interesadas.

La organización puede buscar apoyarse en procesos y tareas automatizadas, buscando siempre la forma de reducir los riesgos.

Incorporar la mejora continua implica:



1. Identificar lo que hay que mejorar:

Identifique y evalúe todos los procesos. Cree prioridades y analice si el proceso impacta en la estrategia general y los objetivos de la organización.

2. Creación de procesos

Estandarice y mapee los procesos de todas las tareas, actividades, personas interesadas, objetivos y todo lo relacionado con la operación de la empresa.



2. Creación de procesos



3. Seguimiento de la mejora

Cree métricas y KPI's (indicadores de rendimiento) para medir con datos reales los resultados de la mejora. De esta forma será más fácil la comparación y el análisis de las versiones, para saber realmente que resultados se obtuvieron y si hay más puntos de mejora.



4. Adoptar métodos de mejora continua

Adopte métodos que optimicen los procesos y ayuden con la mejora continua, como:

4. Adoptar métodos de mejora continua

- **El ciclo PDCA**

Método norteamericano que pone en práctica la filosofía de la mejora continua. 4 pasos que deben realizarse cíclicamente, donde es posible identificar el problema, analizarlo, crear un plan de acción, ejecutar, verificar, normalizar y actuar para mejorar.

1. *Plan* (planificar)
2. *Do* (hacer)
3. *Check* (verificar)

4. Act (actuar)

Ciclo PDCA



© T-CERT®

Ciclo Deming PDCA y el SGSI



© T-CERT®

- **Lean Manufacturing**

Sistema de producción japonés de gestión y mejora de los procesos que implica una fabricación ajustada. Supone reducir los residuos, los costos y encontrar procesos de producción más eficaces.

- **Kaizen**

Metodología japonesa de mejora continua, que reconoce la mejora constante de los procesos, productos o servicios. Kaizen en japonés significa “mejora”.

- **Six Sigma**

Estrategia de gestión que entiende que las producciones tienen variaciones y es necesario eliminar estas fuentes de variabilidad. Six sigma sigue las fases denominadas DMAIC: definir, medir, analizar, mejorar, controlar.

El proceso de mejora significa integrar de manera sistemática los procesos de mejora del SGSI dentro de los procesos normales de revisión de una organización.

Se considera importante que en las reuniones de revisión el SGSI tenga un papel importante, para así demostrar el liderazgo efectivo sobre el SGSI y su preocupación en la mejora del sistema y de la seguridad de la información.

En el proceso de mejora continua, están involucrados los procesos de comunicación y establecimiento de la cultura de la seguridad, y se requiere de la participación de todo el personal ya que se considera es un factor crucial en la mejora del SGSI.



Anexo A

Anexo A

1. A5 Controles Organizacionales



Objetivo: Lograr que la actitud integral de la organización hacia la protección de datos sea una amplia gama de políticas, reglas, procesos, procedimientos, estructuras organizacionales y comportamientos individuales.

- 5.1 Políticas de seguridad de la información.
- 5.5.2 Funciones y responsabilidades de seguridad de la información.
- 5.3 Segregación de funciones.
- 5.4 Responsabilidades de la gerencia.
- 5.5 Contacto con autoridades.
- 5.6 Contacto con grupos de interés especial.
- 5.7 Inteligencia sobre amenazas.
- 5.8 Seguridad de la información en la gestión de proyectos.
- 5.9 Inventario de información y otros activos asociados.
- 5.10 Uso aceptable de la información y otros activos asociados.
- 5.11 Devolución de activos.
- 5.12 Clasificación de la información.
- 5.13 Etiquetado de Información.
- 5.14 Transferencia de información.
- 5.15 Control de acceso.
- 5.16 Gestión de identidad.
- 5.17 Información de autenticación.
- 5.18 Derechos de acceso.
- 5.19 Seguridad de la información en las relaciones con proveedores.
- 5.20 Abordar la seguridad de la información en los acuerdos con proveedores.

- 5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC.
- 5.22 Monitoreo, revisión y gestión de cambios de servicios de proveedores.
- 5.23 Seguridad de la información para el uso de servicios en la nube.
- 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.
- 5.25 Evaluación y decisión sobre eventos de seguridad de la información.
- 5.26 Respuesta a Incidentes de seguridad de la información.
- 5.27 Aprender de los incidentes de seguridad de la información.
- 5.28 Recolección de evidencia.
- 5.29 Seguridad de la información durante una interrupción.
- 5.30 Preparación de las TIC para la continuidad del negocio.
- 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.
- 5.32 Derechos de propiedad intelectual.
- 5.33 Protección de registros.
- 5.34 Privacidad y protección de la PII.
- 5.35 Revisión independiente de la seguridad de la información.
- 5.36 Cumplimiento de políticas, reglas y estándares de seguridad de la Información.
- 5.37 Procedimientos operativos documentados.

2. A6 Controles Orientados a las Personas



Objetivo: Definir cómo los empleados interactúan con los datos y entre sí, la empresa puede regular el componente humano de su programa de seguridad de la información. En este conjunto de controles se incluyen la seguridad del personal, la gestión del capital humano y la formación y sensibilización.

- 6.1 Detección.
- 6.2 Términos y condiciones de empleo.
- 6.3 Concientización, educación y capacitación sobre seguridad de la información.
- 6.4 Proceso disciplinario.

- 6.5 Responsabilidades después de la terminación o cambio de empleo.
- 6.6 Acuerdos de confidencialidad o no divulgación.
- 6.7 Trabajo remoto.
- 6.8 Informes de eventos de seguridad de la información.

3. A7 Controles Físicos



Objetivo: Garantizar la seguridad de los activos tangibles, como sistemas de entrada, procesos de disposición de activos y políticas claras de escritorio. Estos son esenciales para la preservación de la confidencialidad.

- 7.1 Perímetros de seguridad física.
- 7.2 Entrada física.
- 7.3 Protección de oficinas, habitaciones e instalaciones.
- 7.4 Monitoreo de seguridad física.
- 7.5 Protección contra amenazas físicas y ambientales.
- 7.6 Trabajar en áreas seguras.
- 7.7 Limpieza del escritorio y limpieza de pantallas.
- 7.8 Ubicación y protección del equipo.
- 7.9 Seguridad de los activos fuera de las instalaciones.
- 7.10 Medios de almacenamiento.
- 7.11 Utilidades de soporte.
- 7.12 Seguridad del cableado.
- 7.13 Mantenimiento del equipo.
- 7.14 Eliminación segura o reutilización del equipo.

4. A8 Controles Tecnológicos



Objetivo: Garantizar que las regulaciones y procedimientos digitales de la empresa cumplan con criterios de configuración, administración y acceso para que la tecnología no presente huecos de seguridad ya sea por acceso no autorizados, fallas de funcionamientos o por mala administración.

- 8.1 Dispositivos terminales de usuario.
- 8.2 Derechos de acceso privilegiado.
- 8.3 Restricción de acceso a la información.
- 8.4 Acceso al código fuente.
- 8.5 Autenticación segura.
- 8.6 Gestión de capacidad.
- 8.7 Protección contra malware.
- 8.8 Gestión de vulnerabilidades técnicas.
- 8.9 Gestión de configuración.
- 8.10 Eliminación de información.
- 8.11 Enmascaramiento de datos.
- 8.12 Prevención de fuga de datos.
- 8.13 Copia de seguridad de la información.
- 8.14 Redundancia de las instalaciones de procesamiento de información.
- 8.15 Registro.
- 8.16 Actividades de seguimiento.
- 8.17 Sincronización de reloj.
- 8.18 Uso de programas de utilidad privilegiados.
- 8.19 Instalación de software en sistemas operativos.
- 8.20 Seguridad de redes.
- 8.21 Seguridad de los servicios de red.
- 8.22 Segregación de redes.
- 8.23 Filtrado web.

- 8.24 Uso de criptografía.
- 8.25 Ciclo de vida de desarrollo seguro.
- 8.26 Requisitos de seguridad de la aplicación.
- 8.27 Principios de ingeniería y arquitectura de sistemas seguros.
- 8.28 Codificación segura.
- 8.29 Pruebas de seguridad en desarrollo y aceptación.
- 8.30 Desarrollo subcontratado.
- 8.31 Separación de los entornos de desarrollo, prueba y producción.
- 8.32 Gestión de cambios.
- 8.33 Información de prueba.
- 8.34 Protección de los sistemas de información durante las pruebas de auditoría.

Glosario

Glosario

Acción Correctiva: Acción para eliminar la causa de una no conformidad y prevenir que vuelva a ocurrir.

Aceptación del Riesgo: Decisión informada en favor de tomar un riesgo particular.

Activos de información: Son datos, documentos, sistemas o dispositivos que tienen valor para su organización y deben protegerse contra el acceso, uso, divulgación, modificación o destrucción no autorizados.

Alcance de la Auditoría: Extensión y límites de una auditoría.

Alta Dirección: Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis del Riesgo: Proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apreciación del Riesgo: Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

Ataque: Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo.

Atributo: Propiedad característica de un objeto que es cuantitativa o cualitativamente distingible por medios humanos o automáticos.

Auditoría: Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma.

Autenticidad: Propiedad consistente en que una entidad es lo que dice ser.

Colectivo que Comparte Información: Grupo de organizaciones que acuerdan compartir información.

Competencia: Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

Comunicación y Consulta del Riesgo: Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las partes interesadas, en relación con la gestión del riesgo.

Confidencialidad: Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Conformidad: Cumplimiento de un requisito.

Consecuencia: Resultado de un suceso que afecta a los objetivos.

Contexto Externo: Entorno externo en el que la organización busca alcanzar sus objetivos.

Contexto Interno: Entorno interno en el que la organización busca alcanzar sus objetivos.

Continuidad de la Seguridad de la Información: Procesos y procedimientos para asegurar la continuidad de las actividades relacionadas con la seguridad de la información.

Contratar Externamente (verbo): Establecer un acuerdo mediante el cual una organización externa realiza parte de una función o proceso de una organización.

Control de Acceso: Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.

Control: Medida que modifica un riesgo.

Controles: Son los pasos que se toman para mitigar los riesgos de los datos del negocio y los activos de información.

Corrección: Acción para eliminar una no conformidad detectada.

Criterios de Auditoría: Referencias que se utilizan para comparar las evidencias de la Auditoría. Se trata de definir lo que se va a auditar.

Criterios de Decisión: Umbrales, objetivos o patrones que se utilizan para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado.

Criterios de Riesgo: Términos de referencia respecto a los que se evalúa la importancia de un riesgo.

Datos: Conjunto de valores asociados a medidas básicas, medida derivadas y/o indicadores.

Desempeño: Resultado medible.

Dirección Ejecutiva: Persona o grupo de personas en la(s) que los órganos de gobierno han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la organización.

Disponibilidad: Propiedad de ser accesible y estar listo para su uso o demanda de una entidad autorizada.

Dueño del Riesgo: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo.

Eficacia: Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados.

Entidad de Confianza para la Comunicación de la Información: Organización independiente que sustenta el intercambio de información dentro de un colectivo que comparte información.

Escala: Conjunto ordenado de valores, continuo o discreto, o un conjunto de categorías a las que se asigna al atributo.

Evaluación del Riesgo: Proceso de comparación de los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

Evento o Suceso de Seguridad de la Información: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política

de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

Fiabilidad: Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

Función de Medición: Algoritmo o cálculo realizado para combinar dos o más medidas básicas.

Gestión de Incidentes de Seguridad de la Información: Procesos para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de la seguridad de la información.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Gobernanza de la Seguridad de la Información: Conjunto de principios y procesos mediante los cuales una organización dirige y supervisa las actividades relacionadas con la seguridad de la información.

Identificación del Riesgo: Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos.

Incidente de Seguridad de la Información: Evento singular o serie de eventos de la seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Indicador: Medida que proporciona una estimación o una evaluación de determinados atributos usando un modelo analítico para satisfacer unas determinadas necesidades de información.

Información Documentada: Información que una organización tiene que controlar y mantener, y el medio en el que está contenida.

Integridad: Propiedad de exactitud y completitud.

Medición: Proceso para determinar un valor.

Medida Básica: Medida definida por medio de un atributo y el método para cuantificarlo.

Medida Derivada: Medida que se define en función de dos o más valores de medidas básicas.

Medida: Variable a la que se le asigna un valor como resultado de una medición.

Mejora Continua: Actividad recurrente para mejorar el desempeño.

Mejora continua: Práctica de gestión enfocada en la mejora constante de procesos operativos, con el objetivo de ser más eficiente y tener un mejor rendimiento.

Método de Medición: Secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un atributo con respecto a una escala especificada.

Métrica: Son los valores expresados numéricamente que sirven para analizar el rendimiento de una determinada acción o proceso dentro de una empresa. Cualquier cosa que se realice dentro del ámbito empresarial y sea medible, es una métrica.

Modelo Analítico: Algoritmo o cálculo que combina una o más medidas básicas o derivadas siguiendo los criterios de decisión a las mismas.

Necesidades de Información: Conocimiento necesario para gestionar los objetivos, las metas, el riesgo y los problemas.

Nivel de Riesgo: Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.

No Conformidad: Incumplimiento de un requisito.

No Repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.

Norma de Implementación de la Seguridad: Documento que especifica las formas autorizadas para satisfacer las necesidades de seguridad.

Objetivo de la Revisión: Declaración que describe lo que se quiere lograr como resultado de una revisión.

Objetivo: Resultado a lograr.

Objeto de Control: Declaración que describe lo que se quiere lograr como resultado de la implementación de controles.

Objeto en Revisión: Elemento específico que está siendo revisado.

Objeto: Elemento caracterizado por medio de la medición de sus atributos.

Organización: Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos.

Órgano de Gobierno: Conjunto de personas que responden y rinden cuentas del desempeño de la organización.

Parte Interesada: Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

Parte Interesada: Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

Política: Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.

Políticas: Es un documento que expresa una instrucción u orientaciones específicas frente a un área o actividad de una organización, generalmente establecido por la dirección, que debe conocerse y cumplirse.

Probabilidad (likelihood): Posibilidad de que algún hecho se produzca.

Proceso de Gestión del riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

Procesos: Son las actividades y operaciones que implican la creación, almacenamiento, transmisión o procesamiento de activos de información.

Proyecto del SGSI: Actividades estructurales llevadas a cabo por una organización para implementar un SGSI.

Recursos (instalaciones) de Tratamiento de Información: Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

Requisito: Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.

Resultados de las Mediciones: Uno o más indicadores y sus correspondientes interpretaciones que abordan una necesidad de información.

Revisión: Actividad que se realiza para determinar la idoneidad, la adecuación y la eficacia del tema estudiado para conseguir los objetivos establecidos.

Riesgo Residual: Riesgo remanente después del tratamiento del riesgo.

Riesgo: Efecto de la incertidumbre sobre la consecución de los objetivos.

Riesgo: El riesgo indica lo que podría pasar si no se protegen los activos adecuadamente.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Sistema de Gestión: Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

Sistema de Información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

Supervisión, Seguimiento o Monitorización (monitoring): Determinación del estado de un sistema, un proceso o una actividad.

Tratamiento del Riesgo: Proceso destinado a modificar el riesgo.

Unidad de Medida: Cantidad concreta, definida y adoptada por convenio, con la cual se comparan otras cantidades de la misma naturaleza a fin de expresar su magnitud con relación a dicha cantidad.

Validación: Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos para una utilización o aplicación específica prevista.

Verificación: Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los requisitos especificados.

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.