

# ISO 27001



## Implementador

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

## Copyright and Disclaimer

Copyright © T-CERT

Miami, Florida

2024

Todos los derechos reservados.

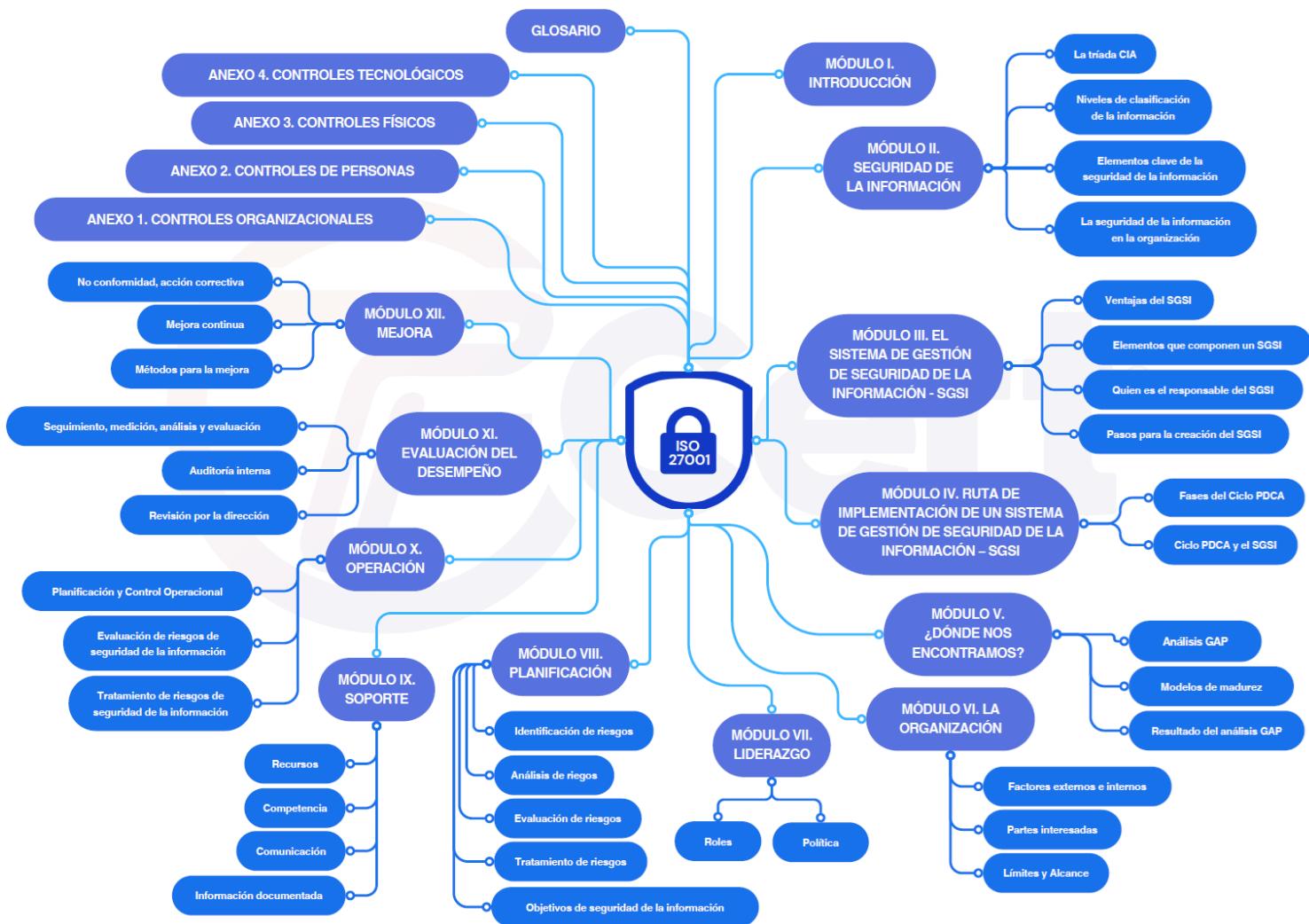
Ninguna parte de esta publicación puede reproducirse, de ninguna forma y por ningún medio, sin el permiso por escrito de T-CERT.

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



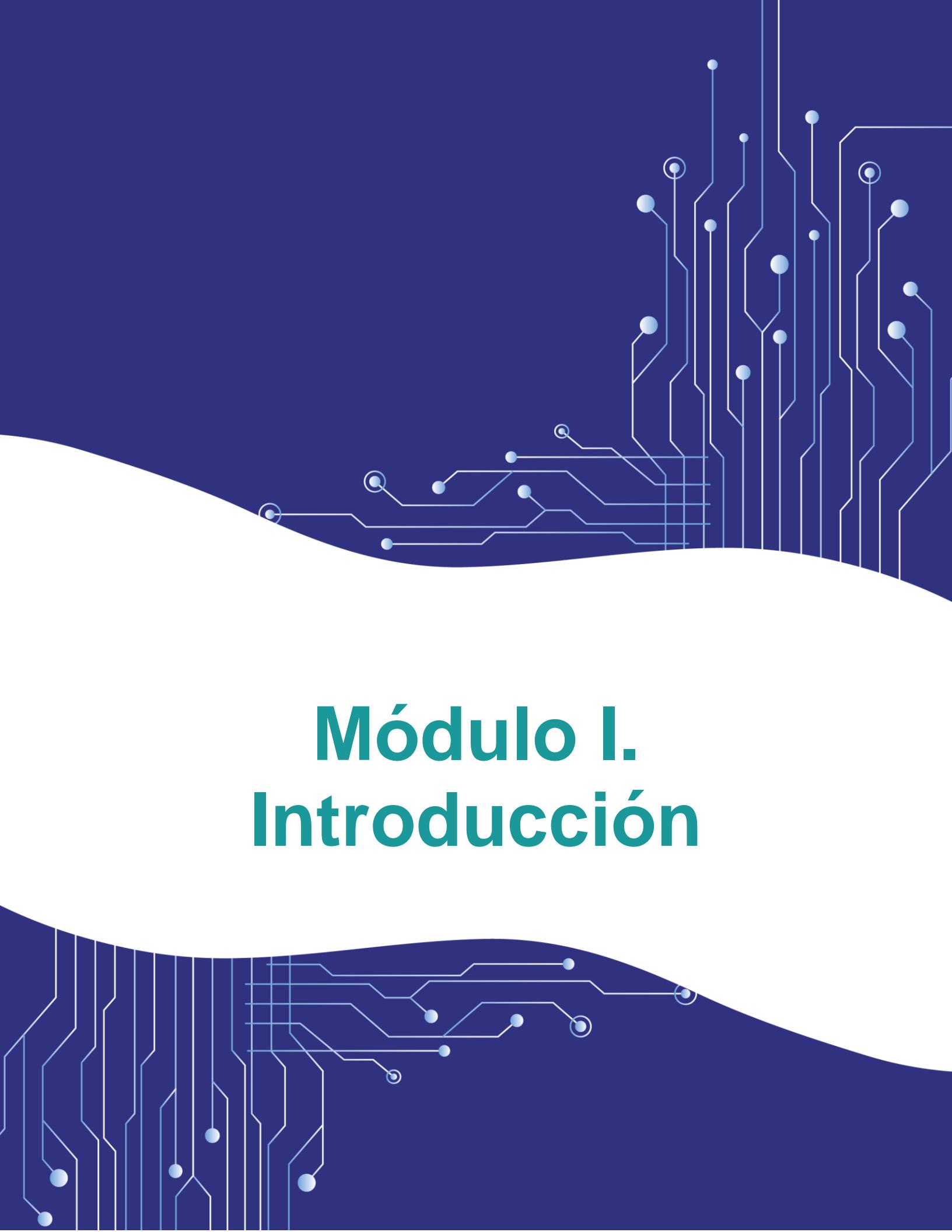
# Contenido

Pág.

<b>Módulo I. Introducción.....</b>	<b>8</b>
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
1.3. Controles .....	14
1.4. ISO/IEC 27003.....	15
<b>Módulo II. Seguridad de la Información.....</b>	<b>17</b>
2.1. La tríada CIA.....	17
2.2. Niveles de clasificación de la información .....	19
2.3. Elementos clave de la seguridad de la información.....	21
2.4. La seguridad de la información en la organización.....	22
<b>Módulo III. El Sistema de Gestión de Seguridad de la Información – SGSI ...</b>	<b>25</b>
3.1. Ventajas del SGSI.....	25
3.2. Elementos que componen un SGSI .....	27
3.3. Quien es el responsable del SGSI .....	28
3.4. Pasos para la creación del SGSI.....	29
<b>Módulo IV. Ruta de implementación de un Sistema de Gestión de Seguridad de la Información – SGSI.....</b>	<b>32</b>
4.1. Fases del Ciclo PDCA.....	32
4.1.1. Planear .....	33
4.1.2. Hacer .....	33
4.1.3. Verificar .....	34
4.1.4. Actuar .....	34
4.2. Ciclo PDCA y el SGSI .....	35
<b>Módulo V. ¿Dónde nos encontramos? .....</b>	<b>37</b>
5.1. Análisis GAP .....	37
5.2. Modelos de madurez.....	37
5.2.1. ¿Qué es la madurez? .....	38

5.2.2. ¿Para qué sirve un modelo de madurez? .....	38
5.2.3. Ventajas del modelo de madurez.....	39
5.2.4. Niveles de madurez .....	39
5.3. Resultado del análisis GAP .....	40
<b>Módulo VI. La organización .....</b>	<b>42</b>
6.1. Factores externos e internos .....	43
6.1.1. Modelo PESTEL .....	43
6.1.2. Análisis FODA .....	45
6.2. Partes interesadas .....	47
6.3. Límites y Alcance .....	48
6.3.1. Consideraciones antes de definir el Alcance del SGSI .....	49
6.3.2. Cómo definir el alcance de un SGSI .....	51
6.3.3. ¿Por qué definir el alcance del SGSI? .....	53
<b>Módulo VII. Liderazgo .....</b>	<b>55</b>
7.1. Política .....	56
7.1.1. Puntos clave en la estructura de la política.....	57
7.1.2. Definir los objetivos de seguridad .....	58
7.1.3. Redactar la política .....	58
7.1.4. Pasos para la definición de la política.....	59
7.2. Roles.....	60
<b>Módulo VIII. Planificación .....</b>	<b>63</b>
8.1. Identificación de riesgos.....	64
8.2. Análisis de riesgos .....	65
8.2.1. Tipos de riesgos .....	65
8.2.2. Clasificación de riesgos .....	66
8.3. Evaluación de riesgos .....	67
8.4. Tratamiento de riesgos .....	68
8.4.1. El plan de tratamiento de riesgos.....	69
8.4.2. La declaración de aplicabilidad – SOA (Statement of Applicability)...	70
8.5. Objetivos de seguridad de la información.....	71
<b>Módulo IX. Soporte .....</b>	<b>74</b>
9.1. Recursos .....	74
9.2. Competencia.....	75
9.3. Comunicación .....	77
9.4. Información documentada.....	78
9.4.1. Niveles de la información documentada .....	79
9.4.1.1. Políticas de Seguridad .....	79
9.4.1.2. Procesos y procedimientos de seguridad.....	80
9.4.1.3. Instrucciones técnicas de seguridad.....	80
9.4.1.4. Registros y evidencias .....	81
9.4.2. Actualización .....	81

9.4.3. Atributos de la información documentada .....	83
<b>Módulo X. Operación .....</b>	<b>85</b>
10.1. Planificación y Control Operacional .....	85
10.2. Evaluación de riesgos de seguridad de la información.....	86
10.3. Tratamiento de riesgos de seguridad de la información .....	88
<b>Módulo XI. Evaluación del desempeño .....</b>	<b>90</b>
11.1. Seguimiento, medición, análisis y evaluación .....	90
11.2. Auditoría interna .....	91
11.3. Revisión por la dirección.....	93
<b>Módulo XII. Mejora .....</b>	<b>98</b>
12.1. No conformidad, acción correctiva .....	98
12.2. Mejora continua .....	100
12.3. Métodos para la mejora .....	103
12.3.1. El ciclo PDCA.....	103
12.3.1. Lean Manufacturing.....	104
12.3.2. Kaizen .....	104
12.3.3. Six Sigma .....	104
<b>Anexo 1. Controles Organizacionales .....</b>	<b>106</b>
<b>Anexo 2. Controles de Personas .....</b>	<b>132</b>
<b>Anexo 3. Controles Físicos .....</b>	<b>140</b>
<b>Anexo 4. Controles Tecnológicos.....</b>	<b>148</b>
<b>Glosario .....</b>	<b>164</b>



# 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 auditoria

## 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.

### 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.



## 6. 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 lograrían. Esto, incluye la selección de controles de seguridad y la elaboración de planes de implementación.



## 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

### 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.

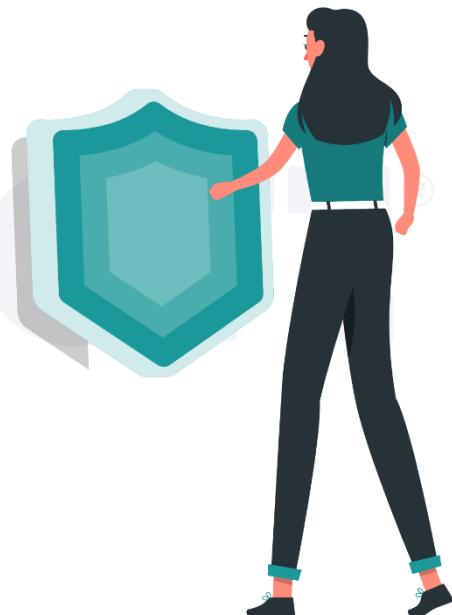
#### **1.2.4. ¿Cómo funciona la norma ISO/IEC 27001?**

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 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.

### 1.3. Controles

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

#### ANEXO A



Son en total 93 controles, referentes a la organización (37), a las personas (8), instalaciones físicas (14) y tecnología (34).

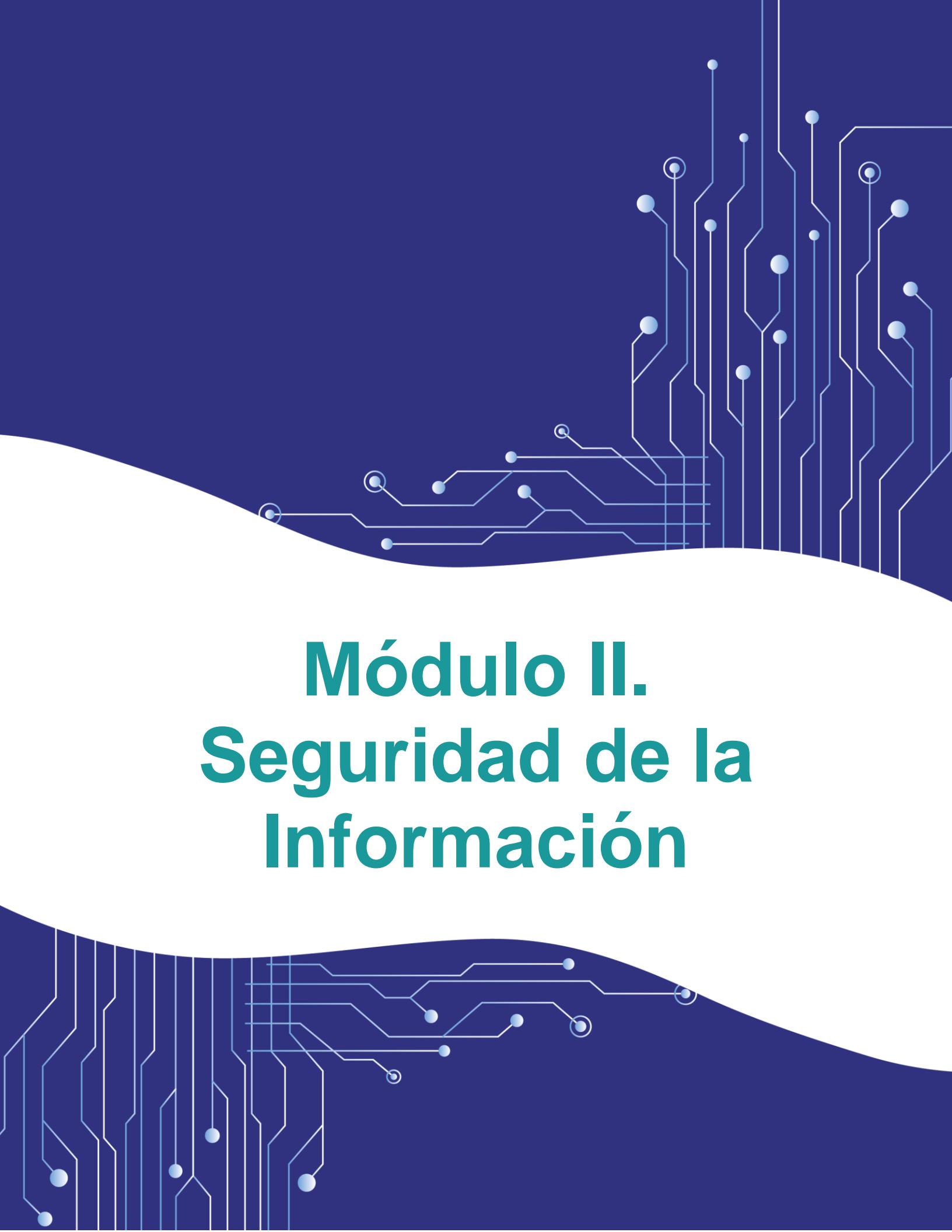
La última versión, permite que cada organización pueda desarrollar atributos propios para los controles de seguridad, facilitando la integración de ISO/IEC 27001

con otros marcos de gobierno y de gestión, así como, la posibilidad de orientar la implantación de los controles a sectores industriales o sectoriales específicos para las actividades propias de cada organización.

#### 1.4. ISO/IEC 27003

Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.





# Módulo II.

# Seguridad de la

# Información

## Módulo II. Seguridad de la Información

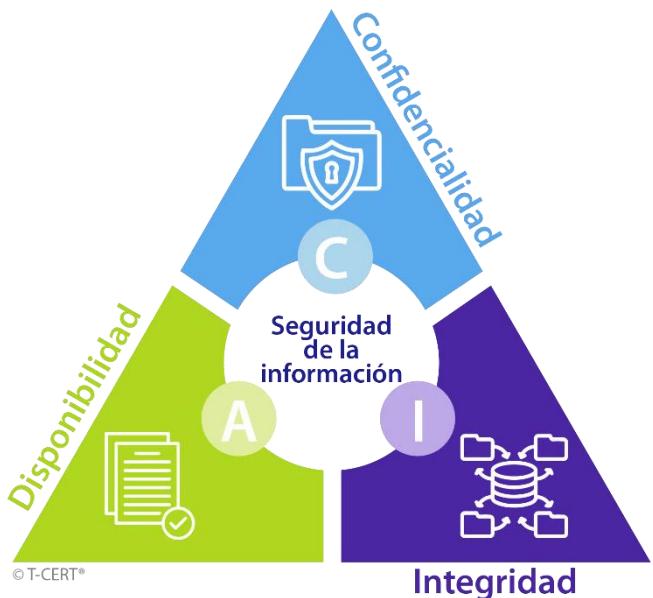
La seguridad de la información es un conjunto de operaciones y métodos, utilizados para proteger y controlar todos los datos que maneja una organización. Además, asegura los datos del uso indebido, accesos no autorizados, robo, interrupción o destrucción durante su ciclo de vida.

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.



#### Personas



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

#### Procesos

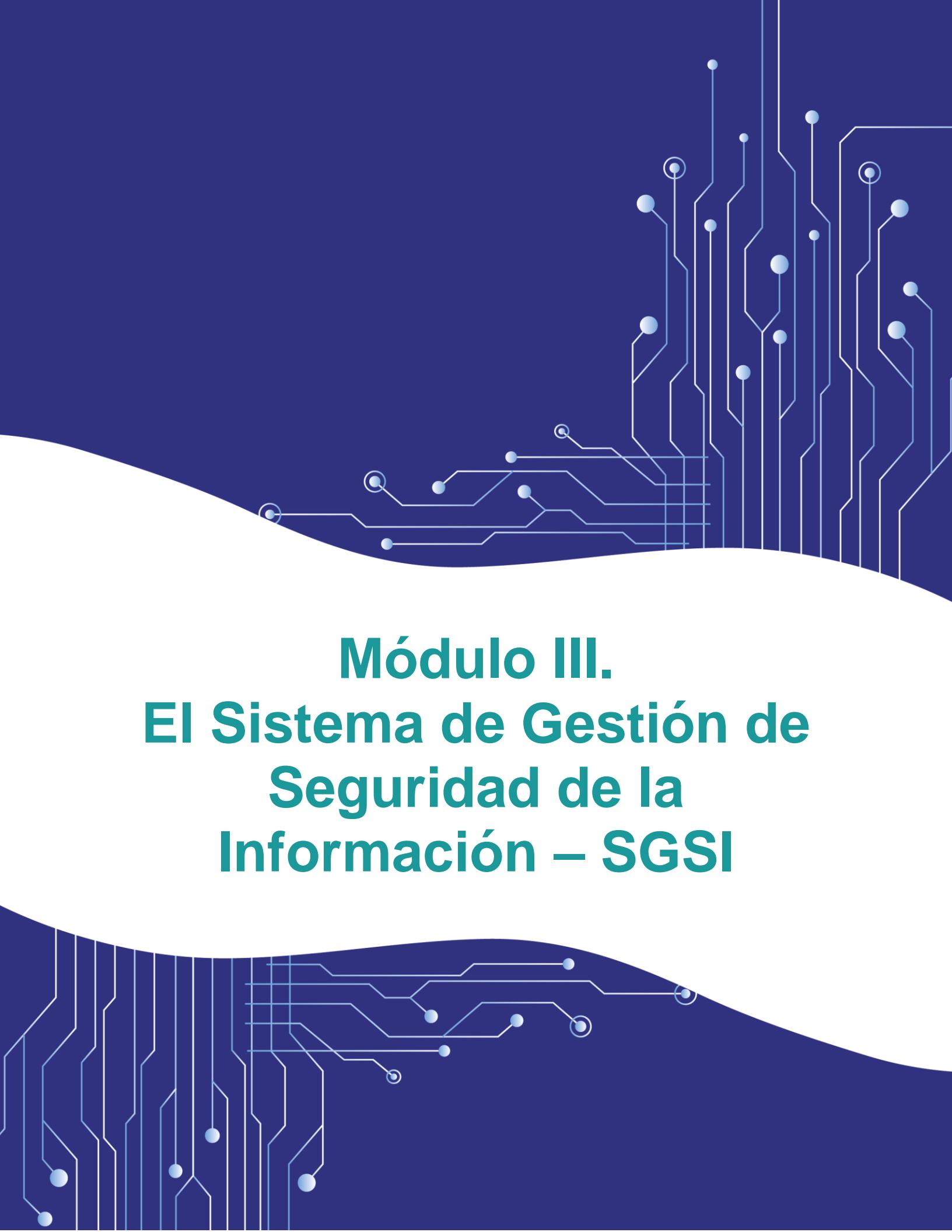


Son todos los mecanismos, sistemas y estrategias orientadas a garantizar la seguridad de la información.

#### 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



## 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:

**Figura 1. Pasos para la creación del SGSI**



© 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.



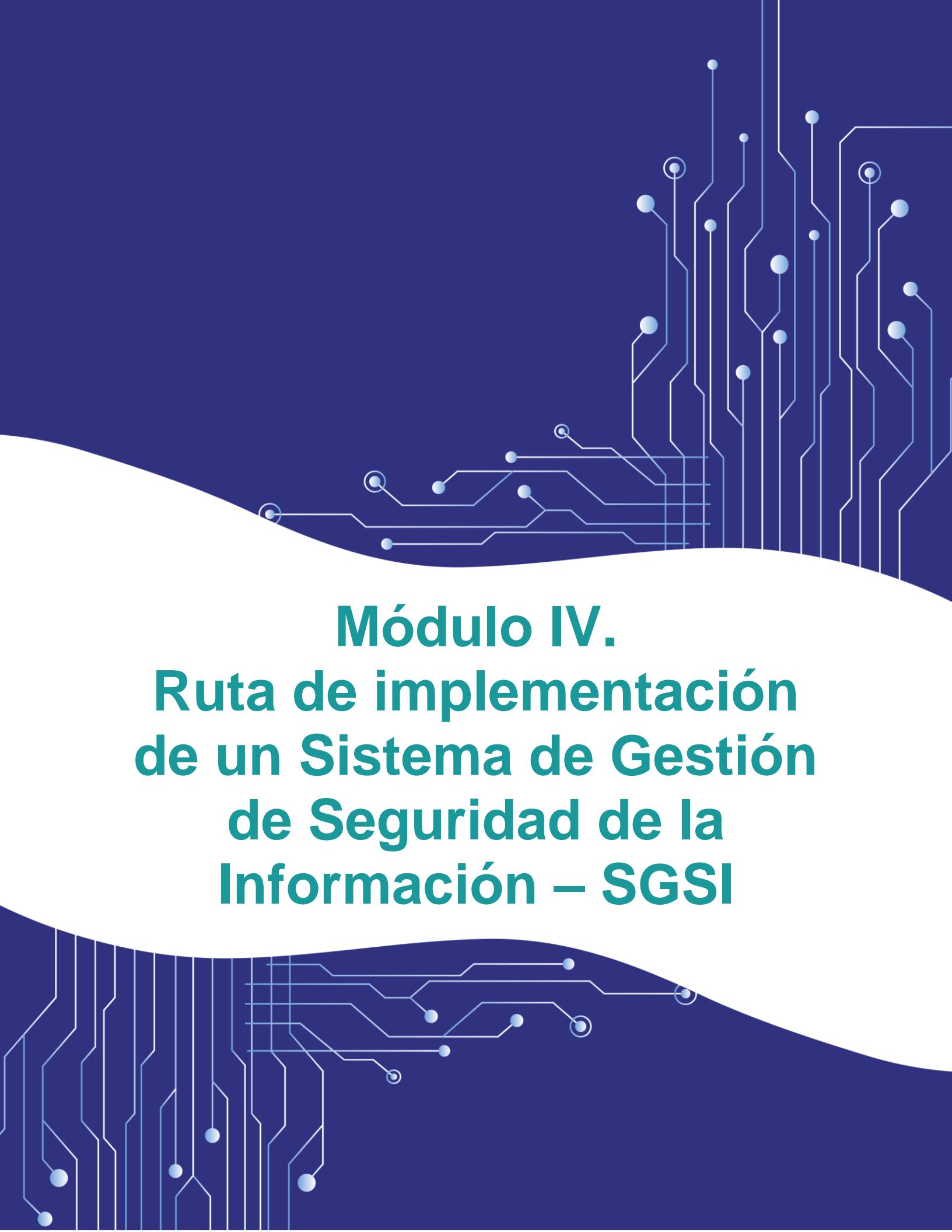
**3. Implementar medidas de seguridad:** Se deben implementar medidas de seguridad apropiadas que resguarden los activos de información. Estas medidas pueden ser técnicas, organizativas o físicas.



**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.**

## **Ruta de implementación de un Sistema de Gestión de Seguridad de la Información – SGSI**

## Módulo IV. Ruta de implementación de un Sistema de Gestión de Seguridad de la Información – SGSI

Para la implantación de un sistema de gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar organizado todo el proceso. El modelo PDCA (Plan, do, check, act), es una estrategia de mejora continua de calidad en cuatro pasos.

### 4.1. Fases del Ciclo PDCA



#### 4.1.1. Planear

En esta etapa se enmarca todo el proceso de análisis de la situación en que actualmente se encuentra la organización respecto a los mecanismos de seguridad implementados, las etapas relevantes de esta fase son:

- Establecer el compromiso con los directivos de la empresa para el inicio, proceso y ejecución.
- Definir el alcance del SGSI.
- Definir las políticas de seguridad.
- Selección y aplicación de una metodología de análisis y evaluación de riesgos.
- Fase de análisis de información de la organización, en esta fase se comprueba cuáles son los sistemas informáticos de hardware y los sistemas de información que actualmente utiliza la empresa para el cumplimiento de su misión u objeto social.
- Fase de evaluación del riesgo; En esta fase se evalúa los riesgos, se tratan y se seleccionan los controles a implementar.



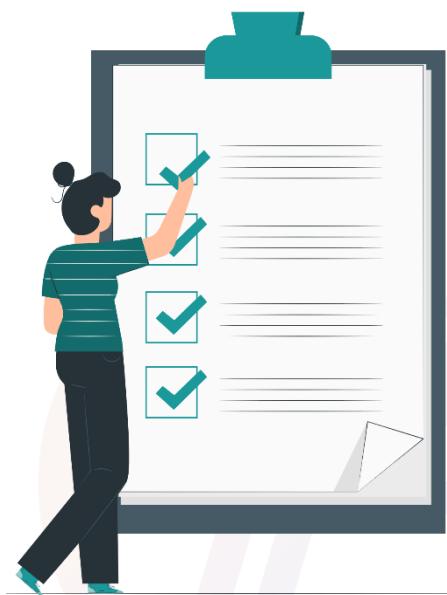
#### 4.1.2. Hacer

En esta fase se hace la implementación de los controles que se definen de acuerdo con el plan de tratamiento de riesgos definidos una vez construida la matriz de riesgos. Las actividades más relevantes de esta etapa son:

- Definir el plan de tratamiento de riesgos.
- Implantar el plan de tratamiento de riesgos.
- Selección e implementación de controles.
- Formación y concientización (a toda la organización).

#### 4.1.3. Verificar

Esta es una fase donde se hace una revisión y evaluación del desempeño de los controles implementados buscan medir la eficacia y eficiencia de los controles seleccionados e implementados. Las etapas de esta fase son:



- Revisión del Sistema de Gestión de Gestión de seguridad.
- Medir la eficacia de los controles seleccionados e implementados.
- Se miden y revisan si existen riesgos residuales.
- Realización de auditorías internas al Sistema de gestión de seguridad de la información.
- Registro de todas las acciones y eventos generados durante las pruebas y validaciones.

#### 4.1.4. Actuar

En este ciclo se requiere una mejora continua, por esta razón en esta fase se busca actualizar o realizar los cambios a los controles identificados en la fase anterior que no están cumpliendo con la eficacia y eficiencia requerida. Las etapas de esta fase son:

- Implantar mejoras al SGSI.
- Definición y aplicaciones de acciones preventivas y correctivas.
- Verificación de la eficiencia de las acciones ejecutadas.

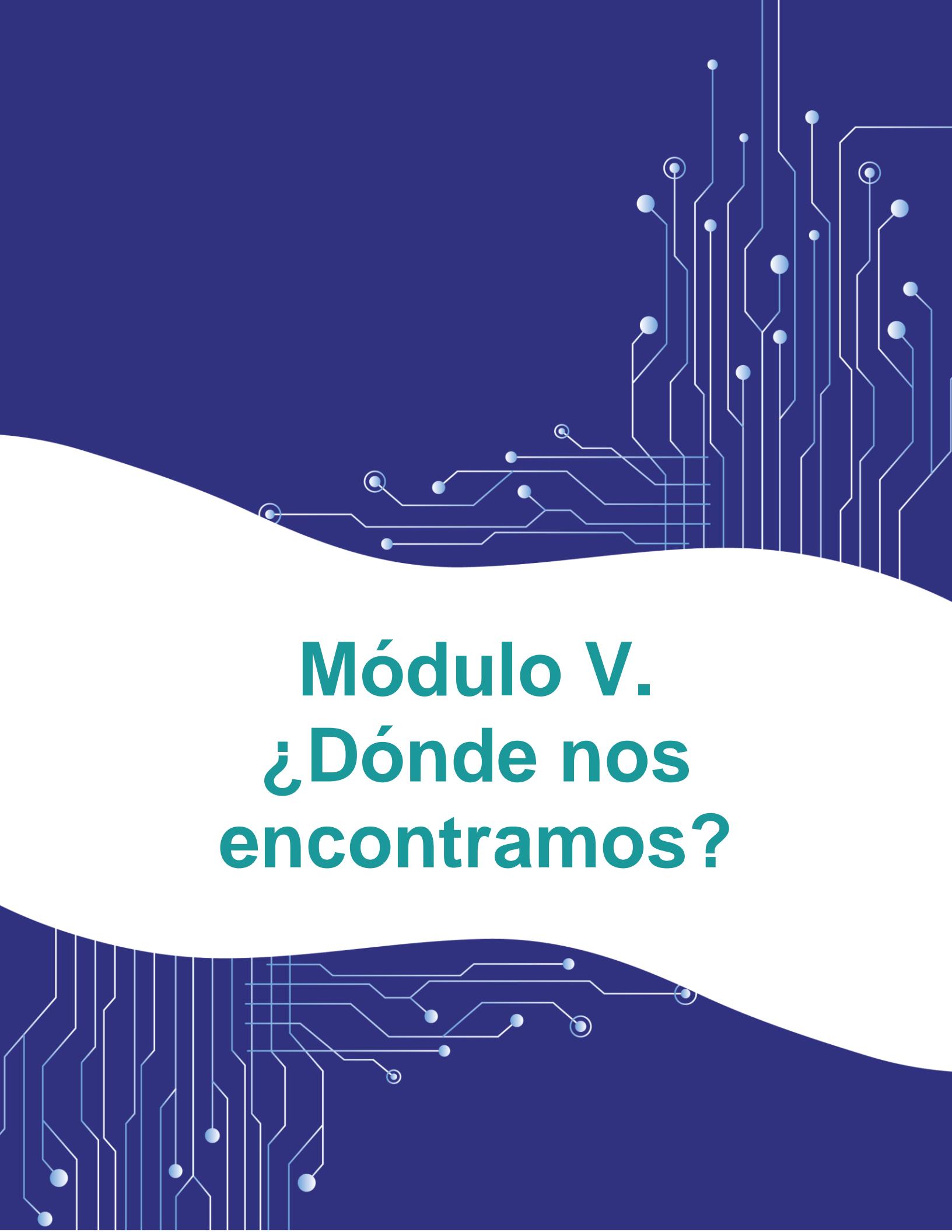
## 4.2. Ciclo PDCA y el SGSI

Para la implementación del SGSI, los pasos serían:

- Planificar: establecer el SGSI
- Hacer: implementar el SGSI.
- Verificar: revisar el SGSI.
- Actuar: mantener y mejorar el SGSI.

### Ciclo Deming PDCA y el SGSI





# Módulo V. ¿Dónde nos encontramos?

## Módulo V. ¿Dónde nos encontramos?

### 5.1. Análisis GAP

Es necesario que la organización entienda sobre su estado actual, saber esto, se puede conseguir con un análisis GAP. El análisis GAP es el punto de partida para la implementación de un Sistema de Gestión de Seguridad de la Información - SGSI.

El análisis GAP es equivalente a una auditoria inicial, en la que se puede entender el grado de implantación de la norma en la organización, cuyos sus objetivos son:



1. Establecer el punto de partida para implementar la norma y evaluar el esfuerzo necesario.
2. Tener una herramienta fiable para elaborar un plan de implementación de ISO 27001.
3. Mantener una herramienta de evaluación del grado de implantación de la norma durante el proceso de implantación y evaluar el grado de avance del proyecto.

### 5.2. Modelos de madurez

Para la realización del análisis GAP ser aconsejable utilizar un modelo de madurez para la evaluación del cumplimiento. Los modelos de madurez más comunes son:

- COBIT Maturity Model
- NIST CSEAT
- CITI ISEM

- CMMI
- CERT/CSO

Estos modelos de madurez son usados como herramientas para la gestión de servicios TI y se utilizan para evaluar qué tan bien se desarrollan los procesos de gestión con respecto a los controles internos.

### 5.2.1. ¿Qué es la madurez?

Es un marco de referencia que permite a las organizaciones evaluar qué tan bien están sus procesos y su nivel de cumplimiento. Las organizaciones con un buen nivel de madurez pueden satisfacer las necesidades de la empresa, funcionar con eficacia y tener flexibilidad para adaptarse a los cambios del entorno empresarial.



### 5.2.2. ¿Para qué sirve un modelo de madurez?

- Permite medir ¿dónde estoy hoy?
- Permite definir dónde debo estar.
- Permite planear lo que debo lograr, para llegar a donde quiero estar.
- Permite gestionar mi crecimiento y evolución.

### 5.2.3. Ventajas del modelo de madurez

Las ventajas de realizar un análisis GAP mediante un modelo de niveles de madurez, son que:



- Proporciona el modelo para un programa de seguridad completo.
- Proporciona la información adecuada a la gerencia del orden en el cual implementar los controles de seguridad.
- Conduce hacia el uso de estándares de mejores prácticas.

### 5.2.4. Niveles de madurez

Los niveles de madurez son un medio para evaluar la adecuación de los controles internos respecto a los objetivos del sistema de gestión.

Con un rango de 0 a 5, las actividades del proceso pueden funcionar en diferentes niveles de capacidad y madurez. El nivel de madurez es una medida de lo bien que un proceso está implementado y funcionando (Elue, 2020). Los niveles son:

- **No existencia (Nivel 0):** no hay reconocimiento de la necesidad del control o requisito.
- **Ad-hoc (Nivel 1):** existe cierto reconocimiento de la necesidad de control interno o requisito. Se aplica para algún problema o tarea específica, no generalizable.
- **Ejecutado (Nivel 2):** los controles existen, pero no están documentados.
- **Definido (Nivel 3):** los controles están en su lugar y están documentados adecuadamente.

- **Manipulable y medible (Nivel 4):** Existe un control interno sobre la aplicación de controles y cumplimiento de requisito.
- **Optimizado (5):** Existe un control interno y continuo sobre la aplicación de controles y cumplimiento de requisitos. Se mide la eficacia de los controles estableciendo objetivos de mejora.

Para establecer el nivel de madurez actual para cada uno de los requisitos y controles de la ISO/IEC 27001 puede realizar un test de cumplimiento, el resultado de esta evaluación indicara a la organización su nivel dentro de una escala según el modelo de madurez definido.

El modelo de madurez COBIT®, se adapta de forma perfecta para establecer un modelo de auditoría que permita medir el nivel de madurez actual respecto a los requisitos de la norma.

### 5.3. Resultado del análisis GAP

El resultado del análisis GAP revelará las buenas prácticas que se tienen frente a los controles internos del SGSI. Para este paso, puede presentar los resultados con evaluaciones parciales por grupos de controles y por control, en donde indique el nivel de cumplimiento de cada uno.





# Módulo VI. La Organización

## Módulo VI. 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.

Es decir, se requiere identificar en qué medida los aspectos internos y externos podrían afectar al propósito de la organización y a su capacidad para lograr los resultados esperados del SGSI.

Se considera importante conocer el punto de vista de las partes interesadas tanto externas como internas, esta es una herramienta que ayuda a identificar causas, riesgos potenciales y aspectos desconocidos sobre la efectividad de las medidas para la seguridad de la información. Por otra parte, generar un plan de comunicación desde una fase temprana ayudará a:

- Obtener un respaldo seguro y el apoyo necesario para los planes de tratamiento de riesgos.
- Identificar riesgos aportados por distintas áreas de experiencia.
- Integrar y comprender los intereses de todas las partes.
- Mejorar la comunicación con las partes internas y externas

Es importante que defina los parámetros externos e internos que deben tenerse en cuenta al gestionar el riesgo.



Analizar estas cuestiones tiene tres propósitos:

1. Comprender el contexto para decidir el alcance del SGSI.
2. Analizar el contexto para determinar riesgos y oportunidades.
3. Garantizar que el SGSI se adapte a los cambios en las cuestiones externas e internas.

### 6.1. Factores externos e internos

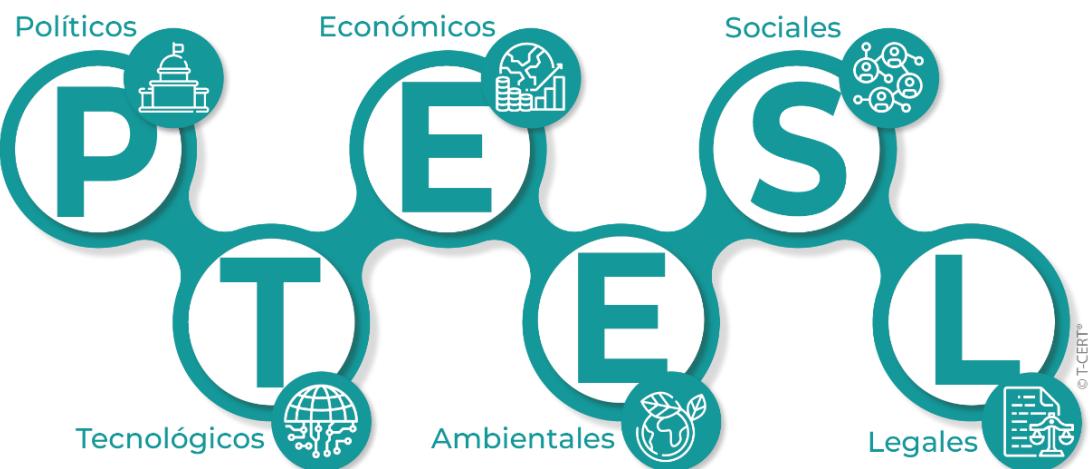
La organización debe establecer las cuestiones externas e internas que son relevantes para su propósito y que afecten a su capacidad para lograr los resultados del SGSI.

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.

#### 6.1.1. 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.



**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.



#### 6.1.2. 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.

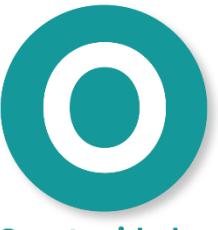
El análisis FODA está diseñado para comprender la situación de la organización a través del análisis de las fortalezas, oportunidades, debilidades y amenazas. Analizar las áreas clave en función de las oportunidades y amenazas, ayudará a obtener la información que se necesita para una toma de decisiones estratégica.





Fortalezas

**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"><li>• ¿Qué es lo que hacemos bien?</li><li>• ¿Qué hace que seamos especiales?</li><li>• ¿Qué es lo que le gusta de nosotros a nuestro público objetivo?</li></ul>	<ul style="list-style-type: none"><li>• ¿Qué decisiones no funcionan bien y por qué?</li><li>• ¿Qué se podemos mejorar?</li><li>• ¿Qué recursos o equipos, pueden ayudar al rendimiento?</li></ul>

	OPORTUNIDADES	AMENAZAS
Factores Externos	<ul style="list-style-type: none"> <li>• ¿Qué podemos usar para mejorar nuestras debilidades?</li> <li>• ¿Hay brechas en nuestros servicios?</li> <li>• ¿Cuáles son nuestros objetivos, en X tiempo?</li> </ul>	<ul style="list-style-type: none"> <li>• ¿Qué cambios en el sector son preocupantes?</li> <li>• ¿Hay nuevas tendencias en el mercado?</li> <li>• ¿En qué es mejor la competencia?</li> </ul>

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

Con el tiempo las cuestiones externas e internas pueden cambiar, por lo que estas y su influencia en el alcance, así como las limitaciones y los requisitos del SGSI deben revisarse periódicamente.

## 6.2. 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.

Es importante identificar las partes interesadas externas, internas y los requisitos de estas partes. Se deben identificar las necesidades, expectativas y requisitos que son relevantes para la seguridad de la información y que pueden cambiar con el tiempo, por lo que su influencia en el alcance, las limitaciones y los requisitos del SGSI deben revisarse periódicamente.

### 6.3. 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.

### 6.3.1. 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 realizados 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.



### 6.3.2. 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



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 con las circunstancias, las amenazas, las tecnologías o los requisitos. Esto puede



## 4. Monitorear y revisar

establecerse dentro de los objetivos de seguridad, determinando los tiempos de aplicabilidad.

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

### 6.3.3. ¿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.

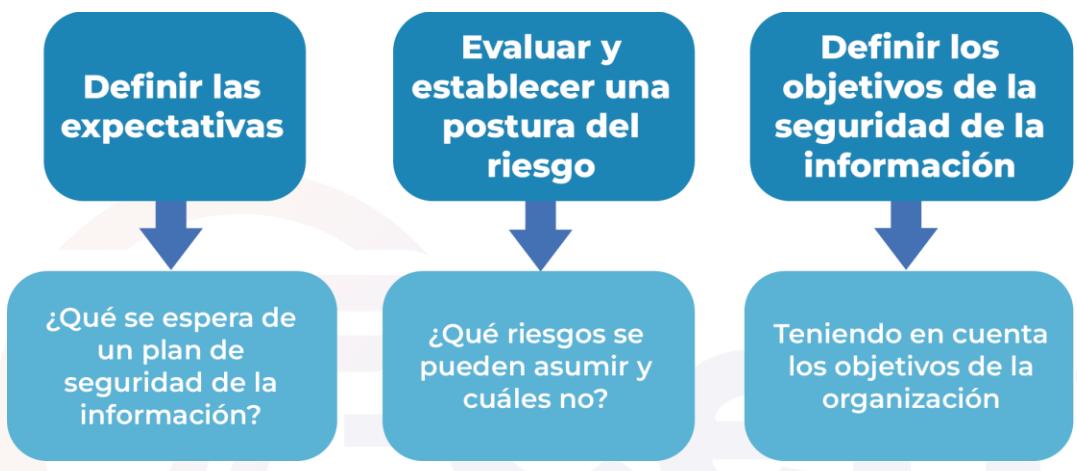




# Módulo VII. Liderazgo

## Módulo VII. Liderazgo

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 debe demostrar su compromiso con respecto al SGSI:

- Garantizando que la política y objetivos del SGSI están establecidos y son compatibles con la dirección estratégica de la organización.
- Garantizando que los requisitos y controles del SGSI están integrados en los procesos de la organización.
- Garantizando la disponibilidad de los recursos que son necesarios para el establecimiento, implementación, mantenimiento y mejora del SGSI.
- Comunicando a toda la organización sobre la importancia de la gestión y del cumplimiento de los requisitos del SGSI.
- Garantizando que el SGSI logre los resultados previstos con el apoyo de la implementación de todos los procesos.
- Dirigiendo y apoyando 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.

## 7.1. Política



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.

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

**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 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.

#### 7.1.1. 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.

### 7.1.2. Definir los objetivos de seguridad

Para definir la política de seguridad de la organización, debe definir claramente los objetivos de seguridad. Estos pueden clasificarse así:

1. **Objetivo 1:** Protección de Activos de Información
2. **Objetivo 2:** Autenticación
3. **Objetivo 3:** Autorización
4. **Objetivo 4:** Integridad de la Información
  - Integridad de los datos
  - Integridad del sistema
  - Irrenunciabilidad de transacciones (No repudio)
  - Confidencialidad
5. **Objetivo 5:** Auditoría de actividades de seguridad.

### 7.1.3. Redactar la política



La política de la seguridad de la información debe ser fácil de entender y se debe explicar de forma resumida para qué sirve la aplicación de esta política de seguridad en la empresa, su utilidad y los responsables.

#### 7.1.4. Pasos para la definición de la política



- **Redacte la política de acuerdo con las necesidades de la organización:** tenga en cuenta el tamaño, la estructura y actividad de cada organización.
- **Tenga en cuenta los objetivos de cada organización:** trate de plasmar en el documento como la seguridad de la información respalda al negocio, en el logro de sus objetivos. Los objetivos deben verse desde un enfoque comercial y desde la seguridad de la información.
- **Demuestre que se tienen en cuenta los requisitos de las partes interesadas:** para este punto es importante que mencione el compromiso de la organización en la satisfacción de estos intereses y de cómo la política de Seguridad e la información contribuye a ello.
- **Comunique la política a las partes interesadas:** Este requisito visibiliza el compromiso de la dirección con el SGSI. Puede nombrar un responsable de realizar esta labor y hacer mención a que se establecerán procedimientos y procesos para garantizar que se realiza en tiempo y formas adecuadas.

- **Defina un propietario de la política:** el propietario se puede encargar de la comunicación y la revisión de la política, incluir este punto ayuda a que la política de la seguridad se mantenga actualizada.

La política de la Seguridad de la Información define lo que se quiere proteger, así como las reglas y conductas para los usuarios del sistema para preservar la seguridad de estos. Además, proporciona una base para la planificación de seguridad incluso cuando se amplían los sistemas o se crean nuevas aplicaciones:

- Describiendo las responsabilidades del usuario, como proteger la información confidencial y crear contraseñas no triviales.
- Explicando cómo controlará la efectividad de sus medidas de seguridad.
- El control y la monitorización nos ayuda a determinar si alguien intenta eludir las salvaguardas para proteger la información.



## 7.2. Roles

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 esté alineada a los objetivos de la seguridad de la información.

La alta dirección no necesita asignar todos los roles, responsabilidades y autoridades, pero si tiene el compromiso de delegar la autoridad adecuada para

hacerlo. La alta dirección debe aprobar los principales roles, responsabilidades y autoridades 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. Este, puede delegar actividades de la seguridad de la información, que pueden incluir:

- Establecimiento, implementación, mantenimiento, informes de desempeño y mejora del SGSI.
- Asesoramiento sobre la evaluación y el tratamiento de los riesgos de la seguridad de la información.
- Diseño de procesos y sistemas de seguridad de la información.
- Establecer pautas sobre la configuración y funcionamiento de controles de la seguridad de la información.
- Gestión de incidentes.
- Revisión y auditoria del SGSI.





# Módulo VIII. Planificación

## Módulo VIII. Planificación

La planificación 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.

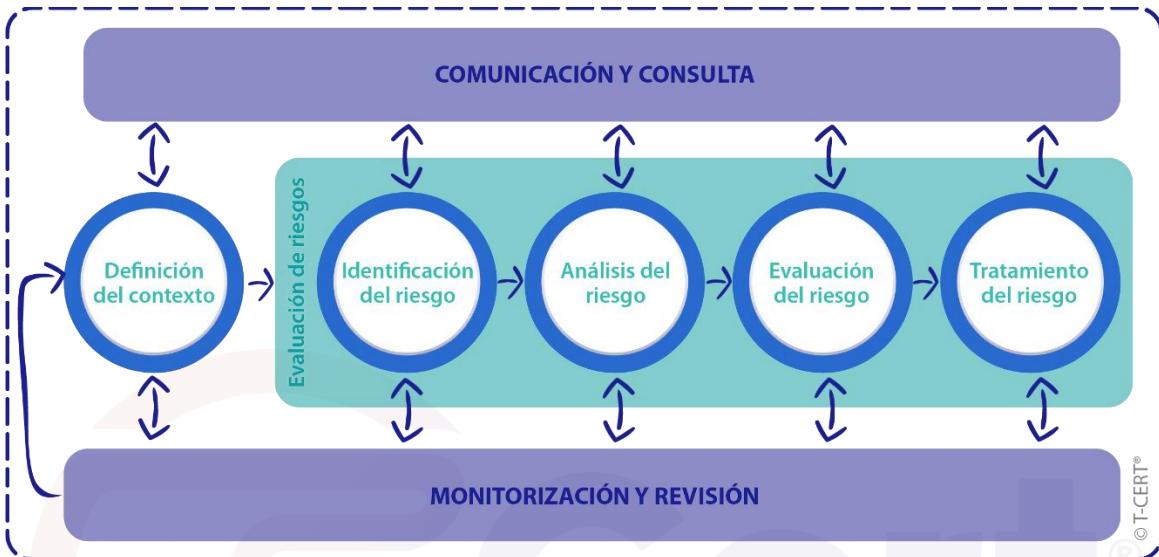


La gestión de los riesgos ayuda a implantar conceptos nuevos dentro del análisis de las vulnerabilidades en la seguridad de la información, fortaleciendo la incorporación de acciones que ayudan no solo a abordar los riesgos, sino también a generar oportunidades. Integrar acciones de evaluación y medición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

## 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.

### 8.1. 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.

## 8.2. Análisis de riesgos

### 8.2.1. 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.



### 8.2.2. 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.

### 8.3. Evaluación de riesgos

La organización evaluará los sucesos de seguridad de la información y decidirá si deben clasificarse como incidentes de seguridad de la información. Para esto establezca:

- Un criterio de priorización de incidentes dependiendo del sistema o servicio afectado, del usuario etc.
- Una evaluación de incidentes, realizada tanto por el usuario como por el equipo de gestión que debe revisar la prioridad.
- Un registro de la evaluación de los incidentes para poder analizar los parámetros de calidad tanto en su resolución como de su clasificación.

Existen diferentes formas para clasificar los riesgos, pero lo habitual es considerar dos parámetros:

1. **Impacto:** Daño causado al negocio (en términos económicos, imagen, etc.).
2. **Urgencia:** La rapidez con la cual la organización necesita corregir el incidente.

La combinación de estos parámetros permitirá determinar la prioridad de cada incidente, de esta manera puede establecer una tabla de valores, así:

**Tabla 2. Ejemplo de tabla de valores**

Urgencia	Nivel de Impacto		
	Alto (3)	Medio (2)	Bajo (2)
Alta (3)	6	5	4
Media (2)	5	4	2
Baja (1)	4	2	1

Clasifique los riesgos en:

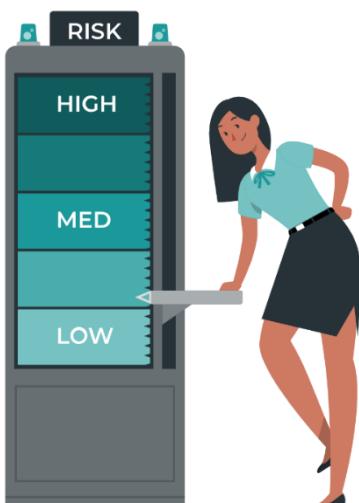
- Nivel crítico (5 a 6) - ROJO
- Nivel grave (3 a 4) – AMARILLO
- Nivel leve (1 a 2) - VERDE

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

#### 8.4.1. 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 3. 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

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



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 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 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.

### 8.5. Objetivos de seguridad de la información

La organización debe establecer objetivos de seguridad de la información en las funciones y niveles pertinentes. 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 IX. Soporte

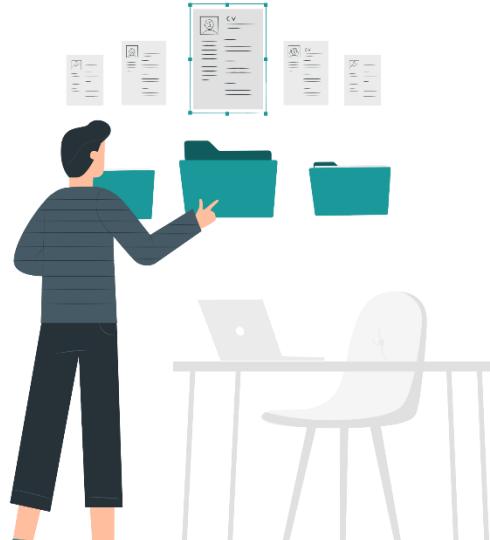
## Módulo IX. Soporte

### 9.1. 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.

## 9.2. 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.

### 9.3. 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.



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.

#### 9.4. Información documentada

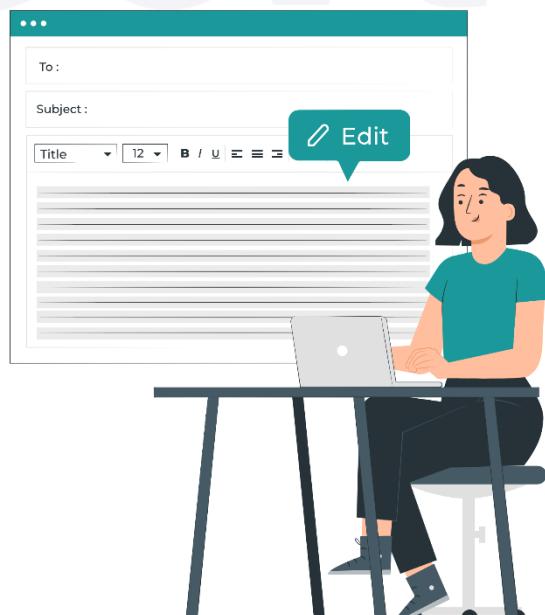
Todo hay que documentarlo, esto es necesario para:

- **Garantizar la repetición en el tiempo de un proceso:** la base para garantizar la aplicación sistemática de un proceso es su documentación.
- **Establecer un proceso de mejora:** la documentación de un proceso permite el acceso a información valiosa cuando se decide evaluar la eficacia del SGSI.

Mantener información documentada es el medio para justificar el cumplimiento con los requisitos de la norma. Si no se crean registros de lo que se hace, no se puede conseguir la mejora continua.

La información del SGSI debe estar disponible para el personal que tenga autorización para su consulta. Los requisitos de la norma piden que:

- La documentación este completa.
- La documentación se encuentre actualizada.



- Se realice un control de la documentación. Para esto es necesario llevar un control mediante que informe cual es la versión actualizada del documento y de las últimas modificaciones.

Los documentos que contienen información importante sobre cómo se gestiona la seguridad de la información deben ser protegidos bajo medidas de seguridad.

#### 9.4.1. Niveles de la información documentada

La documentación del SGSI se puede estructurar en cuatro niveles de información:



##### 9.4.1.1. Políticas de Seguridad

## Políticas de Seguridad

Además de la Política de Seguridad de alto nivel del SGSI, se puede contar con políticas específicas que desarrollen temas particulares.

Se pueden establecer políticas específicas para:

- Uso aceptable de internet dentro de la empresa.
- Uso de dispositivos móviles corporativos.
- Política de uso de dispositivos móviles no corporativos (BYOD o Bring Your Own Device).

#### 9.4.1.2. Procesos y procedimientos de seguridad

### Procesos de Seguridad

Se trata de procesos definidos específicamente para mejorar la eficiencia de las tareas de la Seguridad de la información. El objetivo es gestionar responsablemente los riesgos de seguridad de la información en relación con los tipos de tecnologías que se eligen implementar.

#### 9.4.1.3. Instrucciones técnicas de seguridad

### Instrucciones Técnicas de Seguridad

#### • Procedimientos Técnicos

Por ejemplo:

- El tratamiento de información sensible: se deben determinar requisitos para cualquier tipo de información que sea propiedad, mantenida, utilizada o transmitida por la Organización. Dependiendo de la naturaleza de la información, se establecerán mayores niveles de seguridad aplicables a la información con mayor nivel de sensibilidad.

- Procedimiento para comunicaciones inalámbricas.
- Procedimiento para Accesos remotos.

- **Procedimientos Físicos**

Por ejemplo:

- Pautas y recomendaciones de seguridad de la sala del servidor.
- Almacenamiento y destrucción de información sensible.

#### 9.4.1.4. Registros y evidencias

## Registros y Evidencias

Se trata de documentos que proporcionan evidencias objetivas de la observación a los requisitos del SGSI.

#### 9.4.2. Actualización



La información documentada puede estar presente en cualquier formato, la organización debe definir los atributos para su información, como lo pueden ser el tipo de documento, el propósito, el alcance, fecha, numero de versión, autor, personas responsables, etc. Esto, ayudará en que no exista más de un documento con la misma información.

Se debe desarrollar e implementar un conjunto adecuado de procedimientos para la

manipulación 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.



#### 9.4.3. Atributos de la información documentada

- Nombre del Proceso
- Dueño o propietario del proceso
- Nombre del Activo
- Descripción del Activo
- Tipo de activo de información / Medio
  - Copia impresa, archivo electrónico: (especificar tipo)
  - Medio / dispositivo extraíble: (especificar tipo)
- ¿Contiene Datos personales?
- ¿Contiene Datos personales Sensibles?
- Confidencialidad (Alta – Media – Baja)
- Disponibilidad (Alta – Media – Baja)
- Integridad (Alta – Media – Baja)
- ¿Quién custodia el Activo? (si no es funcional)
- Periodo de retención de datos
- Nivel de protección Actual

Esta información puede llevarse en el formato que prefiera, pero se recomienda en una estructura de tabla.



# Módulo X. Operación

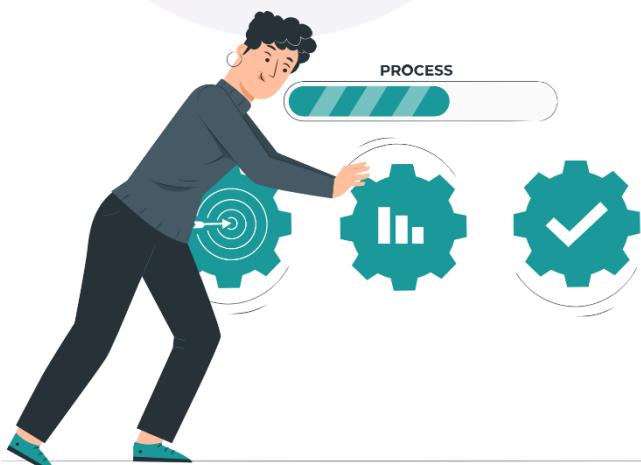
## Módulo X. Operación

### 10.1. Planificación y Control Operacional

La organización debe planificar, implementar y controlar los procesos para cumplir con los requisitos de la seguridad de la información y alcanzar sus objetivos. Sin dejar a un lado que se debe contar con información documentada que garantice la confianza en los procesos, es decir que se llevan acorde a lo planificado.

Es muy importante recopilar toda la información sobre los procesos que utiliza la organización para el cumplimiento de los requisitos de seguridad de la información. De acuerdo con la norma, los procesos para cumplir con los requisitos de seguridad de la información incluyen:

- Procesos del SGSI. Como: revisión por la dirección, auditoría interna, etc.
- Procesos obligatorios para implementar el plan de tratamiento de riesgos de seguridad de la información.



Implementar un SGSI tiene como base los controles de seguridad determinados por la organización, sin dejar a un lado el contexto de la organización, el análisis y evaluación de riesgos y la determinación del alcance o aplicabilidad del SGSI, incluyendo procesos externos.

Es necesario que la organización promueva la mejora continua por medio de la gestión, monitoreo y revisión de los procesos. Además de evaluar las

consecuencias de los cambios planificados o no planificados que deban realizarse en el SGSI, para controlar los efectos adversos.

Para los cambios planificados debe:

- Planificar la ejecución, asignar tareas, responsabilidades, plazos y recursos.
- Implementar los cambios de acuerdo con el plan.
- Supervisar la ejecución de acuerdo con el plan.
- Recopilar evidencias para la información documentada.



Cuando surjan cambios no planificados, debe:

- Revisar las consecuencias.
- Determinar los efectos adversos.
- Planificar e implementar acciones para la mitigación de los efectos adversos.
- Recopilar evidencias de los cambios no deseados y las acciones de mitigación.

## 10.2. Evaluación de riesgos de seguridad de la información

La seguridad de la información es un proceso constante que permite garantizar la mejora continua. Se trata de conseguir progresivamente la mejora en los procesos según las necesidades y posibilidades de la organización.

La organización debe tener un plan programado para evaluar los riesgos de la seguridad de la información, sus resultados pueden generar cambios significativos en el SGSI por lo que la organización debe determinar:

- ¿Cuál de los riesgos o incidentes requieren una evaluación adicional?
- Como se desencadenan las evaluaciones

**NOTA:** Se debe realizar una evaluación de los riesgos de seguridad de la información mínimo una vez al año.

Es importante realizar una evaluación de los riesgos de la seguridad de la información, dentro del cronograma que la organización tenga definido para esto. Las evaluaciones son esenciales para el tratamiento de los riesgos y para la evaluación del desempeño del SGSI. Establecer criterios de evaluación, mediciones claras y concisas permitirán:



- Comunicar los objetivos al personal.
- Planificar su implementación.
- Medir la eficacia de los controles adoptados.
- Implementar cambios a medida que surgen problemas.
- Proponer mejoras y cambios en la gestión de riesgos para mejorar el sistema SGSI.

### 10.3. Tratamiento de riesgos de seguridad de la información

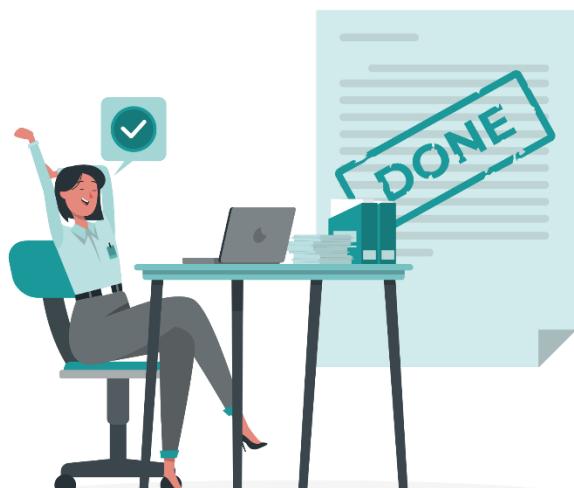
El tratamiento de riesgos debe realizarse después de cada iteración del proceso de evaluación de riesgos de la seguridad de la información. Es decir, siempre que se actualice la evaluación de riesgos la organización se debe aplicar y actualizar el plan del tratamiento de riesgos.

Para desarrollar un plan de tratamiento de riesgos y la implementación de controles y procesos de seguridad es fundamental asignar tareas y responsabilidades. Asignar un responsable, permitirá:

- Establecer los objetivos de las medidas de seguridad
- Hacer efectivas las medidas organizativas
- Implantar y ejecutar las tareas técnicas planificadas.
- Supervisar las actividades
- Recabar y analizar la información de los indicadores.
- La detección y notificación de las incidencias

Para hacer efectivo el tratamiento de riesgos puede generar modelos o plantillas que ayuden en la recolección de información sobre el proceso de implantación de controles y las medidas de seguridad que se derivan del tratamiento de riesgos.

Cuando un proceso se ha definido, planificado, tiene responsables, se encuentra integrado a los procesos de la organización y se ha integrado por un periodo de tiempo para la toma de efectividad, se puede decir que se ha pasado la primera fase de la implementación.





# Módulo XI. Evaluación del desempeño

## Módulo XI. Evaluación del desempeño

La organización debe llevar a cabo una evaluación de rendimiento de la seguridad de la información y de la eficiencia del SGSI. 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.

### 11.1. Seguimiento, 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. El seguimiento y la medición deben realizarse para lograr los objetivos definidos.

Evalué solo lo realmente necesario, es decir, solo supervisé y evalué los recursos que cumplan con el requisito de evaluar la seguridad de la información y la eficiencia del SGSI. Existen dos tipos de medidas:



- **Mediciones de desempeño:** estos expresan los resultados planificados de acuerdo con la actividad, estos pueden ser cantidad de personas, cumplimiento o grado de implementación de controles.
- **Mediciones de eficacia:** estos expresan el efecto de la realización de las actividades planificadas sobre los objetivos de la seguridad de la información.

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.

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.

## 11.2. 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.

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.

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, métodos, al alcance de la auditoría y procesos para manejar la confidencialidad, para garantizar que se cumplen los objetivos.



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 realizará la auditoría (inicio y fin).
- Qué y a quién se va a auditar.
- Donde se realizará la Auditoría.

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. La organización debe:

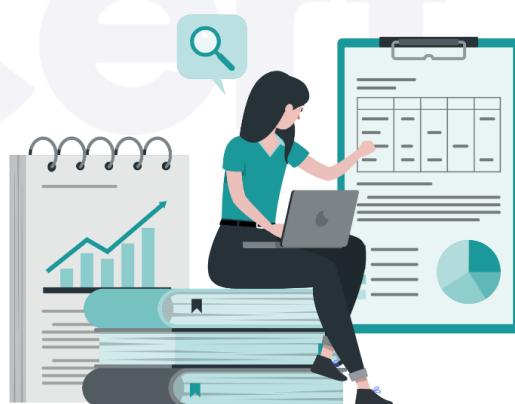
- Identificar los requisitos de competencia de sus auditores.
- Seleccionar auditores internos o externos con la competencia adecuada.
- Contar con un proceso para supervisar el desempeño de los auditores y los equipos de auditoría.
- Incluir en los equipos de auditoría interna personal que tenga conocimientos adecuados sobre seguridad de la información y específicos del sector.

Al realizar una auditoría el líder del equipo auditor debe preparar un plan de auditoría, teniendo en cuenta los resultados de auditorías anteriores y el seguimiento de las no conformidades y riesgos. El equipo auditor debe revisar:

- La adecuación y eficiencia de los procesos y controles.
- El cumplimiento de los objetivos de seguridad de la información.
- El cumplimiento de los requisitos de la norma.
- La coherencia de la Declaración de Aplicabilidad con respecto al resultado de riesgos de la seguridad de la información.
- La coherencia en el plan de tratamiento de riesgos.
- La relevancia e impactos de los aportes tras la revisión por la dirección.

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

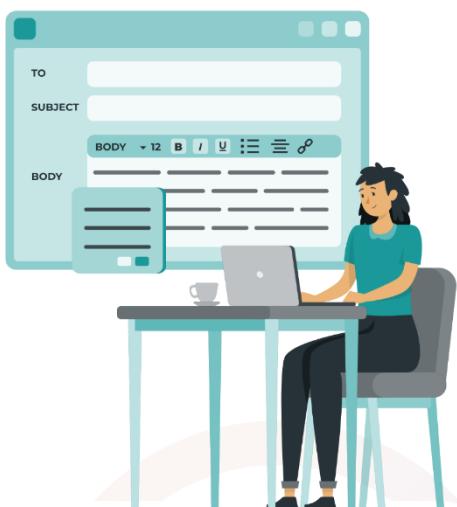
Los resultados del plan de auditoría y los registros recopilados durante las actividades, deben guardarse como información documentada, tanto del plan de Auditoría como del registro del desempeño del SGSI, garantizando el cumplimiento de los objetivos.



### 11.3. 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.



Restrinja en lo posible 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. Estas revisiones al SGSI pueden ser llevadas a cabo por comunicación electrónica o verbal.

El objetivo de la revisión del SGSI por la dirección implica:

- Garantizar que el SGSI y sus objetivos continúen siendo adecuados y efectivos
- Revisar la validez de los problemas identificados y los riesgos de la organización.

Se trata de evaluar los resultados de la gestión para permitir a la alta dirección tomar decisiones estratégicas bien informadas que tendrán un efecto importante en la seguridad de la información y en la forma en que la organización la gestiona.

La dirección debe garantizar que cuando revisa los resultados de la evaluación de riesgos y el tratamiento del SGSI, confirma que los riesgos residuales cumplen los criterios de aceptación de riesgos y que el plan de tratamiento de riesgos esta abordando los riesgos que son relevantes, así como las opciones para su tratamiento.

La revisión por la dirección puede incluir:

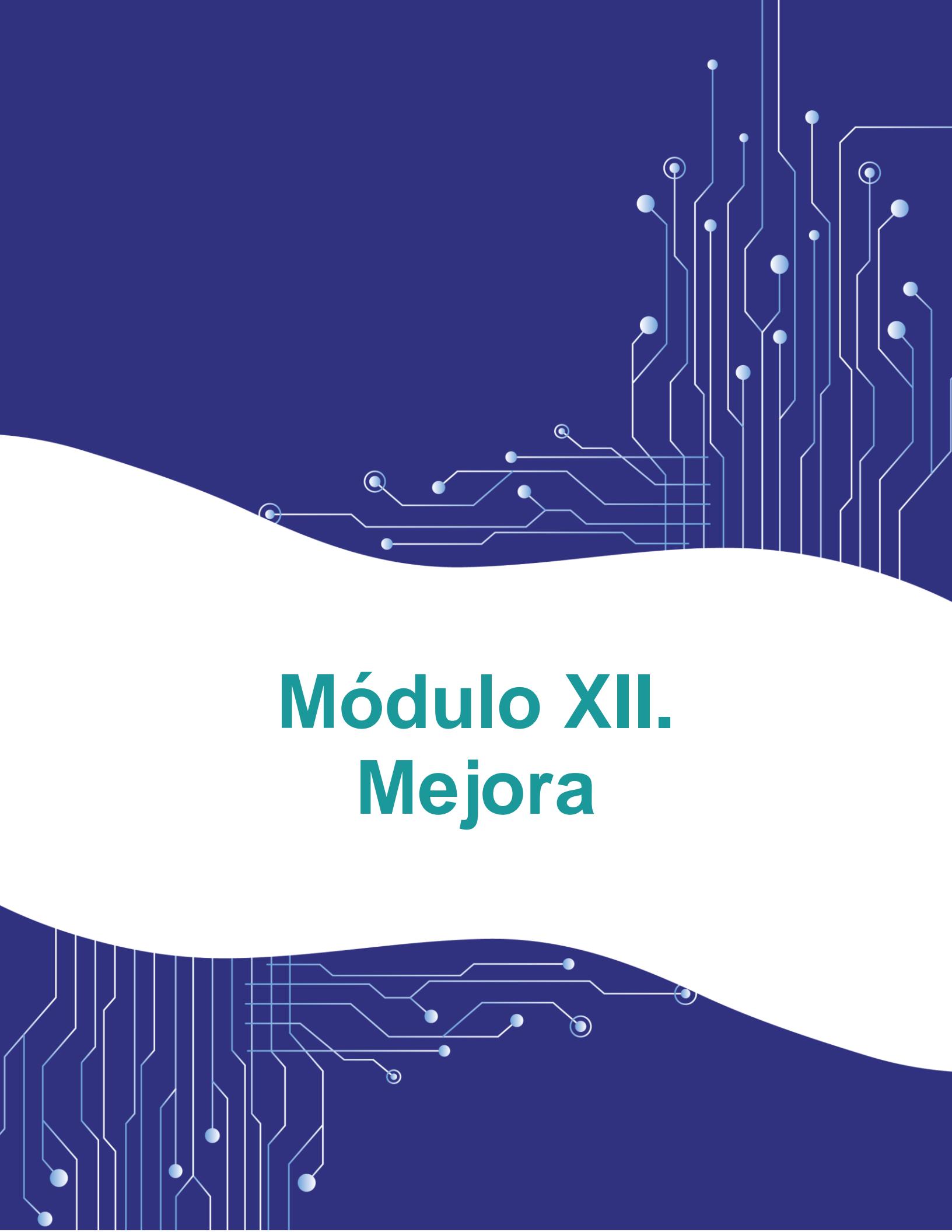
- Revisión de las Revisiones anteriores:
  - Revisar informes de reuniones anteriores.
  - Verificar el estado de las acciones.
  - Registrar el estado de acciones completadas vs acciones en curso.
  - Cerrar las acciones que han sido completadas.
- Revisión de cuestiones internas y externas.
- Revisión del el 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.

Los resultados del proceso de revisión por la dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el SGSI. Además, requiere que se registre la información documentada de las revisiones de gestión, esto con el fin de demostrar que se tienen en cuenta todos los requisitos de la norma ISO/IEC 27001.





# Módulo XII. Mejora

## Módulo XII. Mejora

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.

### 12.1. 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.

Los incidentes de seguridad de la información no necesariamente implican que exista una no conformidad, pero pueden ser un indicador de esta. La reacción ante la no conformidad debe basarse en:

- Identificar el alcance y el impacto de la no conformidad.
- Decidir las correcciones para limitar el impacto de la no conformidad.
- Comunicar el plan al encargado del proceso para que se lleven a cabo las correcciones.
- Ejecutar las correcciones que se hayan decidido.
- Supervisar que se realizan las correcciones, para garantizar efectos secundarios no deseados.
- Si la no conformidad no se corrige, deben tomarse medidas adicionales.

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.

Se deben documentar todos los pasos significativos de la gestión de no conformidades y si se inicia, la gestión de acciones correctivas. La información documentada también debe incluir evidencia sobre si las acciones tomadas han logrado o no los efectos previstos.

## 12.2. Mejora continua

Los riesgos a los que se enfrentan los sistemas de información y las formas en que pueden verse comprometidos evolucionan rápidamente, esto hace que las organizaciones y su contexto nunca sean estáticos. Lo que implica que el SGSI no sea perfecto y siempre exista una forma de mejorarlo.

El SGSI trabaja constantemente a través de la mejora continua para que la organización pueda tener un enfoque más proactivo. La alta dirección puede establecer objetivos de mejora continua, por ejemplo, a través de mediciones de eficacia, coste o madurez de los procesos. 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



2. Creación de procesos



3. Seguimiento de la mejora



4. Adoptar métodos de mejora continua

© T-CERT®



### 1. Identificar lo que hay que mejorar

#### 1. Identificar lo que hay que mejorar:

Identifiqué y evalué 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



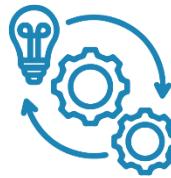
### 3. Seguimiento de la mejora

#### 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.



### 4. Adoptar métodos de mejora continua

La mejora del SGSI implica que todos sus elementos se evalúan teniendo en cuenta las cuestiones internas y externas, los requisitos de las partes interesadas y los resultados de evaluación de desempeño. La evaluación debe incluir el análisis de:

- La idoneidad del SGSI.

- La adecuación del SGSI.
- La eficacia del SGSI.

La mejora continua genera oportunidades de mejora al gestionar no conformidades y acciones correctivas. Cuando se identifiquen estas oportunidades de mejora la organización debe:

- Evaluar la oportunidad y determinar si vale la pena seguir adelante.
- Determinar los cambios al SGSI y los elementos para lograr la mejora.
- Planificar e implementar acciones para abordar las oportunidades.
- Evaluar la eficacia de las acciones de mejora.

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.

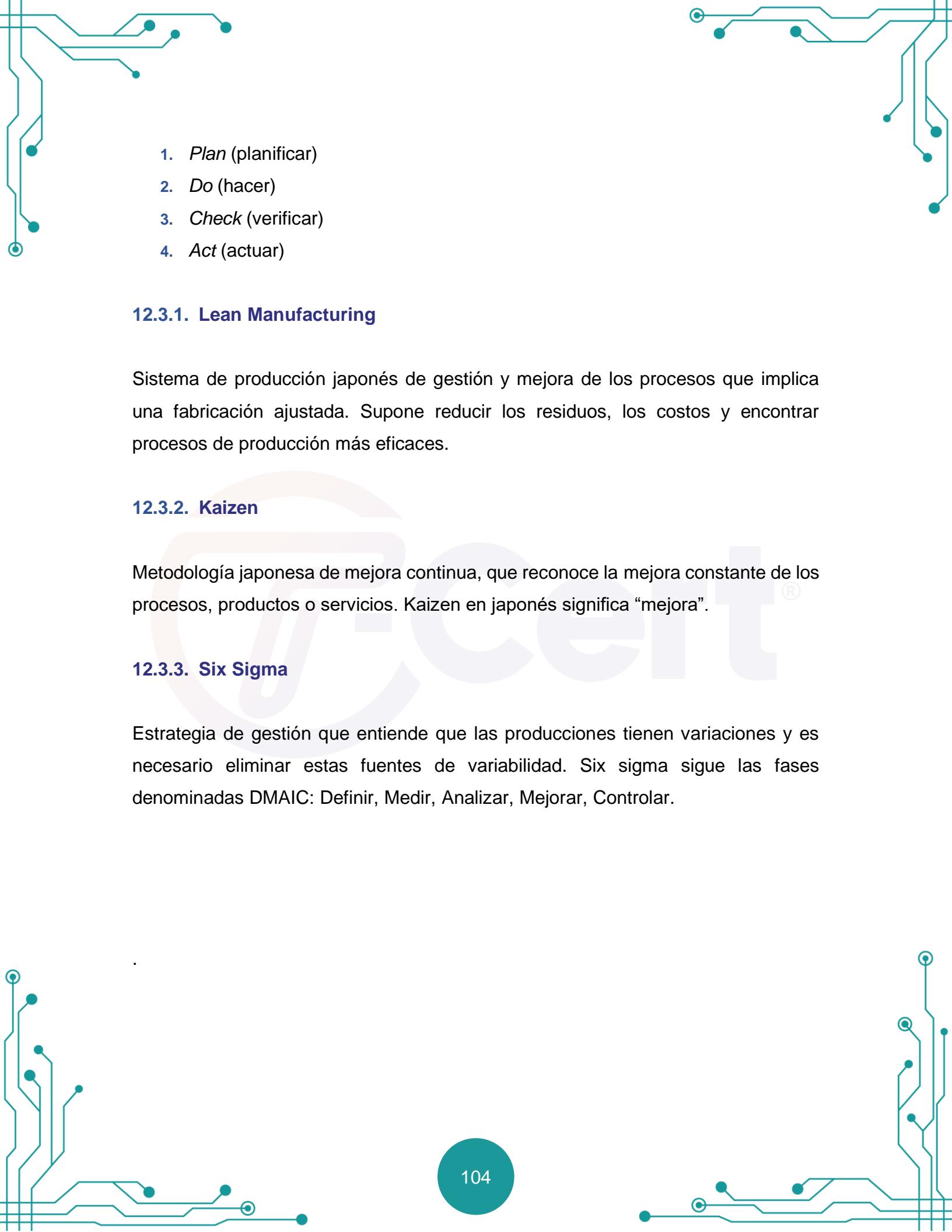
Se considera importante que en las reuniones de revisión el SGSI tenga un papel importante, para así demostrar el liderazgo efectivo sobre el SGSI y su preocupación en la mejora del sistema y de la seguridad de la información.

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.

### **12.3. Métodos para la mejora**

#### **12.3.1. 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)

### 12.3.1. 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.

### 12.3.2. Kaizen

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

### 12.3.3. 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.



# **Anexo 1.**

## **Controles**

# **Organizacionales**

## Anexo 1. Controles Organizacionales

En este anexo podrá profundizar sobre los controles organizacionales del Anexo A de la Norma ISO/IEC 27001.



**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.

### 1. Políticas para la seguridad de la información

La política de seguridad de la información y las políticas específicas de cada tema deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal y las partes interesadas pertinentes, y revisadas a intervalos planificados y si se producen cambios significativos.

Este control requiere que se definan políticas de la seguridad de la información que:

- Sean aprobadas por la dirección
- Se publiquen y se comuniquen a los empleados y partes externas interesadas.

Algunos ejemplos de políticas de Seguridad pueden ser:

- Política de control de acceso
- Política de clasificación y manejo de la información
- Política de seguridad física y ambiental
- Política de temas finales orientados al usuario, tales como:
  - Política de uso aceptable de activos

- Política de escritorio y pantalla limpios
- Política de transferencia de información
- Política de dispositivos móviles y teletrabajo
- Política de restricciones a las instalaciones y uso del software
- Política de copia de seguridad
- Política de transferencia de información
- Política de protección contra software malicioso
- Política de gestión de vulnerabilidades
- Política de controles criptográficos
- Política de seguridad de las comunicaciones
- Política de privacidad y protección de la información personal identificable
- Política de relación con los proveedores

## **2. Funciones y responsabilidades en materia de seguridad de la información**

Las políticas de la Seguridad de la información deben adaptarse continuamente a las necesidades y cambios de la organización, por lo que no pueden permanecer atrasadas. Es decir que, se debe mantener actualizada a política de seguridad de la información.

### **a. Organización interna**

En este apartado, se presentan una serie de requisitos o controles para garantizar que la organización organice las funciones y responsabilidades para gestionar la seguridad de la información.

#### **i. Funciones y responsabilidades de la Seguridad de la información**

Se deben definir las responsabilidades de cada empleado o puesto de trabajo con relación a la seguridad de la información. Es decir que, puede sumar a las funciones

de cada puesto, las funciones que tengan que ver con la seguridad de la información.

Más allá de definir las responsabilidades, estas deben ser comunicadas a cada persona implicada en la seguridad de la información junto a su rol dentro de la organización.

Si se considera necesario involucre a las partes externas que participen en las responsabilidades de la seguridad de la información como los usuarios externos o proveedores.

### 3. Segregación de funciones

Evite el uso y acceso indebido a la información, a las aplicaciones o sistemas que la gestionan (activos de información), por medio de la separación de las funciones asignando distintos perfiles o áreas de responsabilidad.

En ocasiones, no se pueden diferenciar las responsabilidades o tareas por temas de costos, por lo que se puede tener una alternativa para establecer controles que mitiguen los riesgos provocados por la imposibilidad práctica de segregar las funciones, como:

- **Controles de seguimiento y monitorización:** Establecer controles de supervisión de las actividades en tiempo real puede generar una mayor seguridad de que se realizan correctamente.
- **Controles de Auditorías:** Establecer controles mediante registros que revelen los datos necesarios en las auditorías periódicas para evaluar las posibles violaciones de seguridad. También es aconsejable aumentar la frecuencia de las auditorías en temas sensibles con el objeto de transmitir a los empleados la continuidad en la vigilancia de la seguridad de la información.

- **Registros automatizados:** Registrar de forma automática los cambios, accesos o tareas sensibles con la seguridad de la información como la asignación de permisos, contraseñas o modificaciones en aplicaciones de desarrollo.

#### 4. Responsabilidades de la dirección

La dirección requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas específicas de alto nivel y los procedimientos de la organización.

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.

#### 5. Contacto con autoridades

En caso de incidentes en la seguridad de la información puede resultar necesario mantener informados a los organismos de control del estado o administración, como agencias de protección de datos, fuerzas y cuerpos de seguridad del estado, u otros.

Este control debe ser implementado en organizaciones que:

- Mantienen servicios particularmente relevantes para al ámbito público, telecomunicaciones, organizaciones bancarias, servicios de emergencia etc.
- Manejen datos sensibles y cuya difusión indebida o robo pueda causar daños a las personas involucradas.
- Cuando los incidentes contra la seguridad de la información provienen de una fuente externa como Internet y resulte útil o necesario, que varias autoridades y proveedores deban ser llamados a la acción para desviar, suprimir o mitigar la amenaza.

## **6. Contacto con grupos de interés**

La organización establecerá y mantendrá contactos con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

Se trata de mantenerse actualizados en cuanto a las noticias sobre la seguridad de la información y permanecer alerta ante las nuevas amenazas, y si es necesario que se adopte alguna recomendación de estos grupos especializados.

## **7. Inteligencia sobre amenazas**

La organización requiere investigar y recopilar información relativa a las amenazas de la seguridad de la información, después se debe analizar la información recopilada con el fin de generar inteligencia sobre nuevas amenazas que puedan afectar las actividades.

## **8. Seguridad de la información en la gestión de proyectos.**

Para afrontar este requisito puede realizar una evaluación de riesgos, centrada en la seguridad de la información, al comienzo de cualquier proyecto para identificar amenazas, vulnerabilidades y riesgos asociados al proyecto. Esto permitiría adoptar los controles necesarios.

Por otra parte, la organización puede establecer un proceso para integrar la seguridad de la información en cualquier proyecto, que contenga los siguientes pasos:

### **PASO 1. Objetivos de Seguridad**

Debe integrarse como un punto más dentro de las actividades de cualquier proyecto de cara a determinar los objetivos para preservar la confidencialidad, integridad y disponibilidad de la información relacionada o afectada por el proyecto.

## **PASO 2. Evaluación de riesgos**

En la fase de diseño o planificación del proyecto, se debe realizar un análisis de riesgos que permita identificar y ponderar los riesgos asociados a la seguridad de la información.

## **PASO 3. Controles de seguridad**

El paso 2, permitirá tomar las decisiones adecuadas para establecer los controles necesarios para mitigar los riesgos.

## **PASO 4. Proceso de Seguridad de la Información**

Por último, se debe establecer un proceso documentado para integrar la seguridad de la información en cualquier proceso, con el conocimiento de lo que se ha adquirido.

La consideración de la Seguridad de la información en todos los proyectos otorgará a la organización un mayor valor en todos sus proyectos y en su estructura. Adicionalmente, mejora la evaluación de costes, al considerar anticipadamente los riesgos, que después pueden suponer costes no evaluados.

## **9. Inventario de la información y otros activos asociados**

Este control requiere que se elabore y se mantenga un inventario de la información y los activos asociados, incluyendo los propietarios de cada uno.

Se requiere identificar los activos para luego realizar la valoración del riesgo. Se identifican dos clases de activos:

### **1. Primarios**

- Actividades y procesos misionales, tecnología propietaria, aquellos con requisitos legales y contractuales.

- Información de: procesos misionales, de alto costo de procesamiento, almacenamiento, transmisión y recuperación.

## 2. Secundarios

- Hardware.
- Software.
- Redes y conectividad.
- Servicios (Subcontratistas/proveedores/fabricantes).
- Personas a cargo de toma de decisiones (Conocimiento del negocio).

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

Se determinarán, documentarán y aplicarán normas de uso aceptable y procedimientos de tratamiento de la información y otros activos asociados. Este control consiste en:

- Documentar el uso apropiado de la información describiendo los requisitos de seguridad de la información de los activos, instalaciones etc.
- Comunicar a los empleados afectados para evitar el uso indebido.

## 11. Retorno de activos

El personal y otras partes interesadas, según proceda, devolverán todos los activos de la organización que estén en su posesión al cambiar o finalizar su empleo, contrato o acuerdo. Los requisitos para efectuar este control son:

- Formalizar el proceso de finalización de uso incluyendo la cláusula de devolución de activos físicos y/o electrónicos.
- Establecer procedimientos transferencia y borrado de información de forma segura en el caso que sea pertinente (Uso de equipos propios, transferencia y devolución de equipos etc.)

## **12. Clasificación de la información**

La información se clasificará en función de las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.

Existen 4 niveles de clasificación para la información con la que trabajan las organizaciones, independiente de su tamaño, actividad o sector. 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.

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.

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

#### Clasificación de acuerdo con la confidencialidad

<b>Confidencial</b>	Acceso restringido a la alta dirección
<b>Restringido</b>	Directores de área y empleados clave tienen acceso.
<b>Interno</b>	Relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel.
<b>Público</b>	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.

## Clasificación de acuerdo con la Integridad

<b>A (Alta)</b>	Información cuya perdida puede conllevar un impacto negativo de índole legal o económica, retrasar funciones o generar perdidas de imagen severas de la organización.
<b>M (Media)</b>	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>B (Baja)</b>	Información cuya perdida no genera un impacto significativo para la organización o entes externos.
<b>No clasificado</b>	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.

## Clasificación de acuerdo con la disponibilidad

<b>1 (Alta)</b>	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.
<b>2 (Media)</b>	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.
<b>3 (Baja)</b>	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.

## 13. Etiquetado de la información

Se debe aplicar un conjunto adecuado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la 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 en relación a confidencialidad, integridad y 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.

## 14. Transferencia de información

Se deben crear normas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

## 15. Control de acceso

La organización debe definir las normas para el control del acceso físico y lógico a la información y a otros activos asociados, en función de los requisitos de seguridad de la empresa y de la información.

Los propietarios de los activos son los que deben determinar estas normas o políticas de control de acceso de acuerdo con la política de seguridad de la información y el análisis de riesgos. Los principios básicos para la elaboración de estas reglas son:

- La asignación de la menor cantidad de privilegios posibles para llevar a cabo una tarea dentro de un sistema de información.
- La concesión de esos privilegios solamente por el tiempo que sea necesario para el desarrollo de las tareas.

Es decir, se deben asignar los permisos de acceso limitados solamente a la información necesaria para hacer un trabajo, tanto a nivel físico (accesos a instalaciones o soportes de información), como lógicos (Accesos a aplicaciones).

El objetivo de la política de control de acceso debe ser que todo está prohibido a menos que esté expresamente permitido y no al revés. Definir los roles dentro del sistema de Información, ayudara a saber lo que un usuario está autorizado a hacer dentro de un sistema y de lo que no le está permitido.

## 16. Gestión de identidades

Se debe gestionar el ciclo de vida completo de las identidades. Este es un requisito que gestiona la autorización de los usuarios que acceden a los recursos de red. Elabore una política específica para el uso de los recursos de red que contenga los siguientes pasos:

- 1. Identificación:** proporcione una identidad reconocible (por ejemplo, ID usuario o cuenta de usuario, número de seguro social, pasaporte, etc.).
- 2. Autenticación:** garantice que la persona sea quien dice ser (por ejemplo, con el uso de: contraseña, token, huella digital, etc.).
- 3. Autorización:** controle qué acciones puede realizar la persona con su acceso (por ejemplo, con una lista de permisos de materia y lista de permisos de objetos).

La política debe identificar:

- La red y servicios a los cuales se accede.
- Los procedimientos de autorización.
- Que controles tienen estos procedimientos.
- Los medios por los cuales se accede (VPN, Wifi, etc.).
- Los requisitos de autenticación.

- Como se supervisa el uso de los servicios de red.

## 17. Información de autenticación

La asignación y gestión de la información de autenticación, se debe controlar mediante un proceso de gestión, y debe incluir el asesoramiento y capacitación al personal sobre el manejo adecuado de la información de autenticación.

Con respecto a los métodos de autenticación, los siguientes factores se pueden usar, por separado o en combinación:

- **Algo que sabe un sujeto:** como contraseñas y PIN.
- **Algo que tiene un sujeto:** como tarjetas inteligentes, fichas, llaves, etc.
- **Algo que un sujeto es:** como patrones de voz, retina, huella digital, etc.

## 18. Derechos de acceso

Los derechos de acceso a la información y a otros activos asociados deben asignarse, revisarse, modificarse y eliminarse de acuerdo con la política específica de la organización y las normas de control de acceso. Para lograr esto:

- Revise los derechos de acceso a la terminación de empleo o cambios en la organización (cambios de empleo o promociones).
- Limite el tiempo en los derechos de acceso con privilegios especiales.
- Revise las cuentas con privilegios especiales periódicamente y registrar los cambios que se realicen.

## 19. Seguridad de la información en las relaciones con los proveedores

Enumere y aplique procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios del proveedor.

La relación con un proveedor normalmente está regulada por un contrato de prestación de servicios. Es aquí donde se deben indicar las condiciones para el manejo adecuado de la información de la organización.

Lo mejor es acordar las condiciones de seguridad con el proveedor, antes de la firma de los contratos, esto debe quedar documentado ya sea en el contrato o como anexo. Para este control es importante que siga los siguientes pasos:

### Paso 1: Analice los riesgos

Evalué los posibles impactos que puede tener la seguridad de la información en los procesos que impliquen el acceso a la información. Esta es una situación comprometida para la seguridad de la información, con un riesgo potencial de que se produzcan fugas de información, cuyo origen sea el proveedor.

Para evaluar los riesgos, debe analizar qué activos de información estarían afectados por la subcontratación o cesión de datos a terceros y analizar las posibles amenazas y el impacto que tendrían su pérdida de confidencialidad, integridad o disponibilidad.

Se trata de seguir el proceso de evaluación de riesgos para cada activo: aplicación, servicio, tareas o procesos que se hayan subcontratado o se tenga la intención de hacerlo.

## **Paso 2: Selección de controles**

El segundo paso es el análisis o auditoría de los controles que se deben aplicar a los activos identificados para evitar o mitigar los riesgos identificados. Estos controles pueden ser la investigación de los antecedentes de los socios y proveedores, verificando información financiera, antecedentes penales, auditorías de controles y procesos de seguridad del proveedor, etc. Las investigaciones realizadas deben mantenerse dentro de la legalidad vigente y cumplir con las leyes de protección de datos.

## **Paso 3: Acuerdos de Prestación de Servicios**

Una vez identificados los controles de seguridad, enumérelos en los acuerdos de confidencialidad.

## **Paso 4: Control de Accesos**

Defina una política de control y restricción de los accesos a la información. Esta puede ser una herramienta que ayude a mantener el riesgo más controlado evitando en todo momento el acceso a innecesario a la información.

## **Paso 5: Monitoreo**

Supervise y si es necesario audite si se cumplen con todas las cláusulas. Por ejemplo: si se acordó con el proveedor dar el acceso a sus datos solo a un número determinado de sus empleados, esto es algo que debe verificar.

## **Paso 6: Finalización del Servicio**

Defina controles para:

- La devolución de los activos de información.
- La eliminación o destrucción de datos.
- La cancelación y revocación de los accesos.

La finalización de un acuerdo o servicio no supone la finalización de las obligaciones en materia de confidencialidad, esto debe estar contemplado en las cláusulas o anexos del contrato de prestación de servicios.

## **20. Seguridad de la información en los acuerdos con los proveedores**

Defina con cada proveedor los requisitos pertinentes en materia de seguridad de la información, en función del tipo de relación con el proveedor.

Las condiciones de seguridad de la información deben quedar reflejadas en los contratos de forma explícita y en un apartado específico para ello. Los documentos sobre los acuerdos para la seguridad de la información deben estar firmados por ambas partes.

## **21. Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y la comunicación (TIC)**

Defina y aplique procesos y procedimientos para gestionar los riesgos de seguridad de la información, asociados a la cadena de suministro de productos y servicios de TIC.

Para este control, debe tener en cuenta los requisitos de seguridad de la información no solamente de los proveedores, sino también de toda la cadena de suministro. Es decir, los riesgos para la seguridad de la información también se ven afectados por lo que los proveedores de la organización subcontraten. Los principios para sostener una cadena de suministro con garantías son:

- Proveedores de confianza.
- Exigir a los proveedores un control de seguridad a sus propios proveedores.

## **22. Seguimiento, revisión y gestión de cambios de los servicios de los proveedores**

Supervise, revise, evalúe y gestione periódicamente los cambios en las prácticas de seguridad de la información y la prestación de servicios de los proveedores.

Cuando se modifican los servicios prestados por proveedores se debe:

- Aplicar un análisis de riesgos al nuevo escenario.
- Evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir las nuevas necesidades de seguridad si se estima oportuno.

## **23. Seguridad de la información para el uso de servicios en nube**

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se establecerán de acuerdo con los requisitos de seguridad de la información de la organización.

## **24. Planificación y preparación de la gestión de incidentes de seguridad de la información**

La organización debe planificar y prepararse para gestionar los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, funciones y responsabilidades de la gestión de incidentes de seguridad de la información.

## 25. Evaluación y decisión sobre sucesos relacionados con la seguridad de la información

La organización evaluará los sucesos de seguridad de la información y decidirá si deben clasificarse como incidentes de seguridad de la información. Establezca:

- Un criterio de priorización de incidentes dependiendo del sistema o servicio afectado, del usuario etc.
- Una evaluación de incidentes, realizada tanto por el usuario como por el equipo de gestión que debe revisar la prioridad.
- Un registro de la evaluación de los incidentes para poder analizar los parámetros de calidad tanto en su resolución como de su clasificación.

Hay muchas formas de clasificar incidentes, pero lo habitual es considerar dos parámetros:

3. **Impacto:** Daño causado al negocio (en términos económicos, imagen, etc.).
4. **Urgencia:** La rapidez con la cual la organización necesita corregir el incidente.

La combinación de estos parámetros permitirá determinar la prioridad de cada incidente, de esta manera puede establecer una tabla de valores, así:

### Ejemplo de tabla de valores

Urgencia	Nivel de Impacto		
	Alto (3)	Medio (2)	Bajo (2)
Alta (3)	6	5	4
Media (2)	5	4	2
Baja (1)	4	2	1

Clasifique las incidencias en:

- Nivel crítico (5 a 6) - rojo
- Nivel grave (3 a 4) – amarillo
- Nivel leve (1 a 2) - verde

## 26. Respuesta a incidentes de seguridad de la información

Se trata de controlar el proceso de resolución de incidentes en la seguridad de la información, para esto:

- Evalué si la organización tiene la capacidad para resolver el incidente por si misma o necesita ayuda de terceros.
- Mantenga un registro con las evidencias de las incidencias.
- Establezca el sistema de comunicaciones necesarias entre usuarios y el equipo de gestión de incidencias o quien deba estar informado de las actuaciones y situación del proceso de resolución de las incidencias.
- Registre las acciones llevadas a cabo y los resultados de las mismas.
- Cierre la incidencia formalmente cuando se haya resuelto.
- Realice un análisis para determinar las causas de cada incidente.

## 27. Aprender de los incidentes de seguridad de la información

Los conocimientos obtenidos de los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información. Los incidentes no solo son un problema a solucionar, sino una fuente de información para la resolución de futuros incidentes o para la mejora de la seguridad de la información.

Mantenga una base de conocimientos sobre los incidentes en la seguridad de la información con:

- La creación de un registro que considere:
  - Volumen de incidentes producidos
  - Tipología de incidentes producidos
  - Coste de la resolución de la incidencia
  - Impacto de la incidencia
  - Solución aplicada

La información sobre los incidentes puede ayudar a:

- Identificar los incidentes más recurrentes y de alto impacto.
- Mejorar el sistema de gestión con nuevos controles y criterios para la evaluación de riesgos.
- Realizar entrenamientos a los usuarios para evitar incidentes y a los gestores de incidentes para mejorar la resolución de los mismos. Para este punto se recomienda utilizar datos No reales para los entrenamientos.

## 28. Recopilación de pruebas

Los incidentes sobre la seguridad de la información pueden requerir acciones posteriores, como sanciones o acciones legales. Para este control, es importante conservar la información sobre las incidencias de forma se pueda rescatar los datos de:

- Los inicios y cierres de sesión.
- Las identificaciones.
- El estado de los dispositivos y de las redes.
- Las evidencias de reuniones informativas, documentación sobre responsabilidades y funciones de seguridad del personal.

## **29. Seguridad de la información durante las perturbaciones**

La organización debe planificar cómo mantendrá la seguridad de la información en un nivel adecuado, durante una interrupción.

## **30. Preparación de las TIC para la continuidad de la actividad**

La preparación de las TIC se planificará, aplicará, mantendrá y probará en función de los objetivos de continuidad de las actividades y los requisitos de continuidad de las TIC.

La continuidad del negocio debe tener en cuenta el tiempo requerido para realizar restauraciones completas del sistema, lo que puede requerir una operación diversa en varios sitios.

## **31. Requisitos legales, estatutarios, reglamentarios y contractuales**

Se requiere que se identifiquen, documenten y mantengan actualizados los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir estos requisitos.

## **32. Derechos de propiedad intelectual**

Este control requiere que se apliquen procedimientos que garanticen el uso del software de acuerdo a los términos de la Ley de Propiedad Intelectual. Para esto, tenga presente y responda:

- ¿Disponemos de una política de uso legal de productos Software?
- ¿Aseguro la no violación de derechos de copia?

- ¿Dónde compro los productos Software?
- ¿Mantengo la política de licencias del Software comprado?
- ¿Controlo el número máximo de usuarios por licencia?
- ¿Reviso periódicamente que se estén utilizando solamente productos Software con licencia?
- ¿Cumplio con los derechos de copia de material audiovisual, libros, informes etc.?
- ¿He comunicado al personal la política de uso legal de software aclarando que cosas están permitidas y cuáles no?
- ¿He advertido al personal sobre las consecuencias de la violación de las políticas de uso legal de software estableciendo las medidas disciplinarias oportunas?
- ¿He identificado los activos de información que están afectados por derechos de propiedad intelectual?
- ¿Se mantiene la documentación que justifique o acredite la propiedad de las licencias (discos, manuales etc.)?

### 33. Protección de documentos

Los registros se deben proteger contra la pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada. Se trata de clasificar los registros de información y aplicar los controles necesarios según los requisitos legales.

Para cumplir con la protección de los documentos, debe revisar el cumplimiento con:

- La definición y publicación de las directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información.
- El mantenimiento de un calendario de retenciones donde se identifique los registros y los períodos de tiempo que deben retenerse.
- El inventario de los registros de información clave o crítica.

### **34. Privacidad y protección de la Información Personal Identifiable - PII**

La organización identificará y cumplirá los requisitos relativos a la preservación de la privacidad y la protección de la Personal Identifiable Information - PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

### **35. Revisión independiente de la seguridad de la información**

El enfoque de la organización para gestionar la seguridad de la información y su aplicación, incluyendo personas, procesos y tecnologías, se revisarán de forma independiente a intervalos planificados, o cuando se produzcan cambios significativos.

### **36. Cumplimiento de las políticas, reglas y normas de seguridad de la información**

Se requiere una revisión periódica del cumplimiento de la política de seguridad de la información de la organización, así como de las políticas, reglas y normas específicas de la alta dirección. Los responsables de cada área deben revisar que los procedimientos de la organización sean aplicados de acuerdo a los requisitos definidos, para esto los responsables deben:

- Determinar la forma de revisar cómo se cumplen los requisitos de seguridad de la información definidos en las políticas, normas y en otras regulaciones aplicables.
- Tener en cuenta la implementación de sistemas de medición automática y herramientas de informes.

Cuando se identifiquen incumplimientos se deberá:

1. Identificar las causas.

2. Evaluar la necesidad de tomar medidas.
3. Implementar las acciones correctivas apropiadas.
4. Revisar la eficacia de las acciones correctivas.
5. Identificar las deficiencias y debilidades del sistema.

Lleve registros documentados de los resultados de las revisiones y de las acciones correctivas realizadas.

### **37. Procedimientos operativos documentados**

Los procedimientos operativos de las instalaciones de tratamiento de la información deben documentarse y ponerse a disposición del personal que los necesite.



# **Anexo 2.**

## **Controles de**

## **Personas**

## Anexo 2. Controles de Personas

En este anexo podrá profundizar sobre los controles de personas del Anexo A de la Norma ISO/IEC 27001.



**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.

### 1. Proyección

Las comprobaciones de los antecedentes de todos los candidatos a personal se llevarán a cabo antes de su incorporación a la organización y de forma continuada, teniendo en cuenta las leyes, reglamentos y normas éticas aplicables, y serán proporcionales a los requisitos de la empresa, la clasificación de la información a la que se va a acceder y los riesgos percibidos.

Se establecen controles para la verificación de los antecedentes de los candidatos a un empleo. La aplicabilidad de este control tiene que ver con:

- Los requisitos del negocio en cuanto a las funciones que va a desempeñar el candidato y los requisitos definidos para el puesto en relación a la Seguridad de la información
- La clasificación de la información a la que va acceder el candidato y los riesgos asociados

Una de las limitaciones para implementar este control son las leyes o normas vigentes relacionadas con la protección de datos personales y el tratamiento ético en los contratos.

### 1.1. Selección

En el proceso de selección se pueden aplicar una serie de controles para verificar temas de seguridad, así como la formación y experiencia del contrato. La norma propone una serie de medidas, la organización debe realizar una evaluación sobre la necesidad de aplicarlas.

- **Medidas de Seguridad den el proceso de Selección de personal:**
  - Comprobar las referencias profesionales.
  - Comprobar las referencias personales.
  - Comprobar la veracidad del currículum vitae del aspirante.
  - Confirmar las calificaciones académicas y profesionales señaladas.
  - Comprobar de forma independiente la identidad (DNI, pasaporte, etc.)
  - Comprobaciones en detalle: Antecedentes penales, disciplinarios, etc.
- **Competencias en Seguridad de la información:**
  - Comprobar si tiene la capacitación necesaria para desempeñar sus funciones (formación, experiencia).
  - Verificar en lo posible el perfil del candidato en relación a su confiabilidad si va a desempeñar una tarea sensible para la organización en materia de Seguridad de la Información.

Por otro lado, se pueden definir controles similares antes de firmar un contrato con un tercero o contratista. Además, se deben tener presente, las medidas para la seguridad de la información análogas en los procesos de promoción dentro de la organización.

## **2. Términos y condiciones del empleo**

Este control solicita incluir en los contratos con los empleados y contratistas, las obligaciones y responsabilidades ligadas a la Seguridad de la Información.

Mantener informadas a las personas sobre las condiciones de trabajo, es una muy buena práctica, además de una medida preventiva de conductas indebidas para la seguridad de la información. Algunas medidas que propone la norma se pueden tener en cuenta si son aplicables:

- Todos los empleados y contratistas con acceso a información sensible deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información.
- Los empleados y contratistas deben estar informados de sus responsabilidades y derechos legales tales como las relativas a derecho de copia o legislación de protección de datos.
- Los empleados y contratistas deben tener información de sus responsabilidades para:
  - La clasificación de información.
  - La gestión de activos de información.
  - Las instalaciones de procesamiento de información.
  - Los servicios de información a los que accede.
  - El manejo de información de otras organizaciones o partes externas.
- Los empleados y contratistas deben estar informados de las acciones a ser tomadas si el empleado o contratista desatiende los requisitos de la seguridad de la organización.

## **3. Concienciación, educación y formación en seguridad de la información**

El personal de la organización y las partes interesadas pertinentes recibirán una concienciación, educación y formación adecuadas en materia de seguridad de la

información, así como actualizaciones periódicas de la política de seguridad de la información de la organización y de las políticas y procedimientos específicos de cada tema, según corresponda a su función laboral.

La norma brinda indicaciones de aspectos que deben incluirse en la formación y sensibilización, como:

- La formación debe incluir el compromiso de la dirección con la seguridad de la información en toda la organización.
- La importancia del conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información contenida en las políticas, normas, contratos etc.
- La responsabilidad de los empleados y contratistas de sus propias acciones u omisiones en la protección de la información
- Los procedimientos básicos de la seguridad de la información, por ejemplo:
  - Procedimiento de notificación de incidentes de seguridad.
  - Procedimientos sobre uso de contraseñas seguras.
  - Controles sobre software malicioso.
  - Limpieza de escritorios, etc.

#### 4. Proceso disciplinario

Este control propone formalizar y comunicar un proceso disciplinario para los incumplimientos de la seguridad de la información. Estas medidas deben aplicarse contra el personal y otras partes interesadas pertinentes que hayan cometido una infracción de la política de seguridad de la información. El proceso disciplinario debe:

- Asegurarse de que la infracción se ha cometido.
- Evitar tratamientos injustos o incorrectos de los empleados.

- Considerar respuestas graduales tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición.

Tenga en cuenta que un sistema disciplinario no siempre tiene que tener medidas correctivas o negativas. También se puede considerar un sistema disciplinario con medidas positivas que premien el buen desempeño o se establezcan sistemas de que involucren a los empleados.

## 5. Responsabilidades tras el cese o el cambio de empleo

Las responsabilidades y obligaciones en materia de seguridad de la información que sigan siendo válidas tras el cese o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y a otras partes interesadas. El objetivo es proteger la información en un escenario de finalización de contrato o cambio de empleo.

Este control generalmente se pasa por alto y tiene un importante potencial de riesgo para la seguridad de la información y se debe considerar dentro de un SGSI. La norma propone que se incluyan las siguientes cuestiones:

- Incluir en las responsabilidades de la desvinculación requisitos sobre la seguridad de la información, como:
  - Responsabilidades legales cuando sean aplicables o necesarias.
  - Responsabilidades incluidas en los acuerdos de confidencialidad.
- Establecer periodos de vigencia para después de la desvinculación en los términos y condiciones del empleo de:
  - Deberes y responsabilidades que permanecen validos después de la desvinculación.
  - Cambiar o actualizar las responsabilidades en los términos y condiciones del empleo ante cambios de empleo dentro de la organización.

## 6. Acuerdos de confidencialidad o no divulgación

Los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización en materia de protección de la información deberán ser identificados, documentados, revisados periódicamente y firmados por el personal y otras partes interesadas pertinentes.

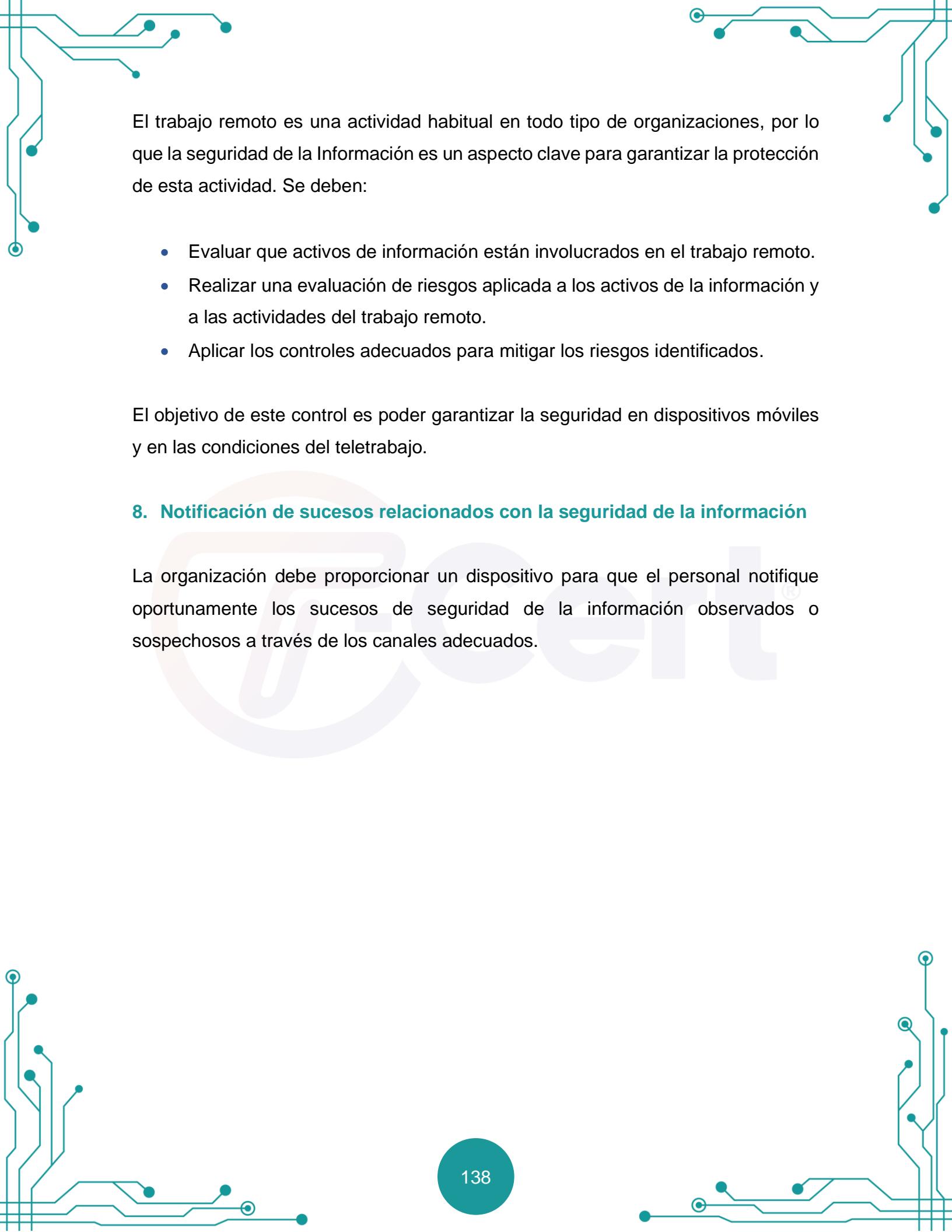
Los acuerdos de confidencialidad afectan tanto a la información propia, como a informaciones que provengan de terceras partes, por lo que se deben considerar acuerdos de confidencialidad tanto a personal propio, como a clientes y proveedores.

Los acuerdos de confidencialidad se deben hacer firmar, en lo posible físicamente, antes de iniciar una transferencia de información. Estos acuerdos deben incluir:

- La naturaleza de la información.
- La duración del acuerdo.
- Los procedimientos de rescisión.
- Las responsabilidades y las propiedades.
- El uso permitido de la información.
- El derecho de auditoría.
- Los procesos a llevar a cabo en caso de una infracción.
- Cláusulas que obliguen a mantener el deber de secreto debe incluso más allá de la relación profesional entre las dos entidades.

## 7. Trabajo remoto

Se requiere aplicar medidas de seguridad cuando el personal trabaje a distancia, para proteger la información a la que se acceda, procese o almacene fuera de las ubicaciones de la organización.



El trabajo remoto es una actividad habitual en todo tipo de organizaciones, por lo que la seguridad de la Información es un aspecto clave para garantizar la protección de esta actividad. Se deben:

- Evaluar que activos de información están involucrados en el trabajo remoto.
- Realizar una evaluación de riesgos aplicada a los activos de la información y a las actividades del trabajo remoto.
- Aplicar los controles adecuados para mitigar los riesgos identificados.

El objetivo de este control es poder garantizar la seguridad en dispositivos móviles y en las condiciones del teletrabajo.

## 8. Notificación de sucesos relacionados con la seguridad de la información

La organización debe proporcionar un dispositivo para que el personal notifique oportunamente los sucesos de seguridad de la información observados o sospechosos a través de los canales adecuados.



# Anexo 3. Controles Físicos

## Anexo 3. Controles Físicos

En este anexo podrá profundizar sobre los controles físicos del Anexo A de la Norma ISO/IEC 27001.



**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.

### 1. Perímetros físicos de seguridad

Se deben precisar y utilizar perímetros de seguridad para proteger las zonas que contengan información y otros activos asociados.

Los requisitos para la seguridad física deben tener en cuenta los niveles de protección del perímetro de las instalaciones o elementos que contienen la información a proteger:

- Muros
- Vallas
- Alarmas
- Suelos
- Protección de ventanas
- Cerraduras, etc.

## 2. Entrada física

Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados. Este control, está orientado a proveer protección contra la entrada no autorizada de:

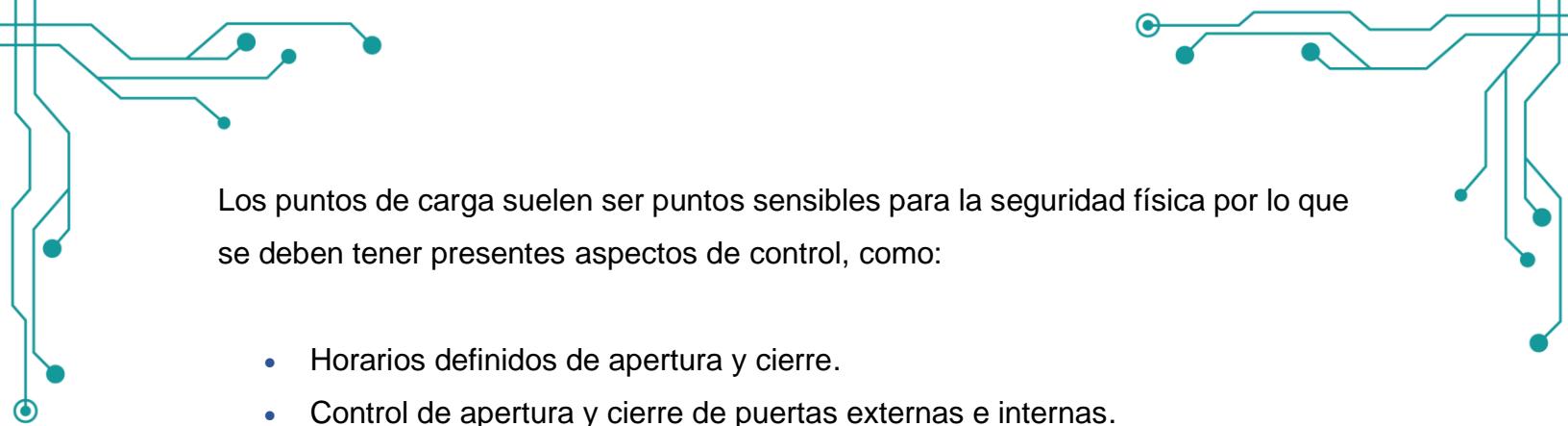
- **Áreas atendidas:** las áreas restringidas a personal autorizado deberían contar con un área de recepción atendida o medios de control adecuados para limitar el acceso físico.
- **Sistemas Antiincendios:** contar con sistemas de protección contra el fuego cumpliendo con la legislación vigente.
- **Detección de intrusión:** Se deben considerar sistemas de detección de intrusos (p ej. Alarmas)
- **Segmentación de espacios:** Separe las áreas de proceso de información que van a ser gestionadas por personal externo de las propias de la organización.

## 3. Seguridad de oficinas, salas e instalaciones

En cuanto a las instalaciones deben diseñarse y aplicarse un nivel de seguridad física, para evitar al máximo posible el riesgo que la información confidencial sea accesible para los visitantes. Se debe considerar la posibilidad de en uso de técnicas de enmascaramiento (masking) de datos referidos a nombres o actividades de clientes.

## 4. Supervisión de la seguridad física

Las áreas específicas deben vigilarse continuamente para evitar accesos físicos no autorizados.



Los puntos de carga suelen ser puntos sensibles para la seguridad física por lo que se deben tener presentes aspectos de control, como:

- Horarios definidos de apertura y cierre.
- Control de apertura y cierre de puertas externas e internas.
- Control de personal.
- Realización de inventarios de materiales entregados.
- Revisión de mercancías entregadas para detectar materiales peligrosos.
- Separar entregas entrantes y salientes.
- Necesidad de informar de cualquier incidente a los responsables de seguridad.
- Barreras adicionales de seguridad.

## 5. Protección frente a amenazas físicas y medioambientales

Debe diseñarse y aplicarse una protección contra amenazas físicas y medioambientales, como catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras. Las leyes exigen tener planes de protección y emergencias, pero se puede buscar un asesoramiento especializado si se considera necesario.

En este control se deben considerar medidas de protección contra inundaciones, incendios y terremotos para mitigar sus efectos.

## 6. Trabajar en zonas seguras

Es necesario crear y aplicar medidas de seguridad para trabajar en zonas seguras, como:

- Prohibición de trabajos sin supervisión por parte de terceros.
- Revisión de las zonas a la finalización de las visitas.

- Prohibición de uso de móviles / cámaras a no ser que estén expresamente autorizados.

## 7. Escritorio y pantalla despejados

Las pantallas no deben mostrar información cuando el equipo no esté en uso y los escritorios deben estar libres de papeles cuando no estén en uso o desatendidos. Esta Una de las políticas de seguridad más fácilmente reconocidas y que más se incumple en la práctica.

## 8. Ubicación y protección de los equipos

Cada equipo debe estar situado en un lugar seguro y protegido, para:

- Evitar accesos no necesarios.
- Proteger los equipos de áreas sensibles como centros de datos o salas de servidores.
- El control de protección en lugares de almacenamiento de equipos si estos contienen información.
- Tener medidas de protección contra daños eléctricos (fuentes de alimentación reguladas, líneas de alimentación separadas y respaldadas etc.)
- Su control medioambiental, cumpliendo con las especificaciones del fabricante en cuanto a condiciones de humedad, temperatura protección contra polvo o materiales que puedan dañar los equipos.
- Poder tener medidas de protección contra radiaciones.

Adicionalmente, se deben establecer pautas de prohibición de comer, beber y fumar cerca del equipo para evitar daños.

## **9. Seguridad de los activos fuera de los locales**

Se deben proteger los bienes que se encuentren fuera de las instalaciones de la organización. Para esto, conserve un registro del cuidado de los activos que abandonan la organización y realice evaluaciones de riesgo para instalaciones donde serán utilizados

## **10. Medios de almacenamiento**

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

## **11. Servicios de apoyo**

Las instalaciones de procesamiento de la información deberán estar protegidas de los cortes de electricidad y otras interrupciones causadas por fallos en los servicios públicos de apoyo.

## **12. Seguridad del cableado**

Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra interceptaciones, interferencias o daños. Se trata de evitar el posible daño de las infraestructuras, como las posibles interferencias que corrompan los datos o el suministro. Puede seguir las siguientes recomendaciones:

- Los cables deben estar bajo tierra hasta el punto de acceso dentro de la instalación, o tener otro tipo de protección.
- Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencias.

- Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos.
- Como medidas adicionales puede realizar barridos técnicos de los cables de comunicación para dispositivos no autorizados (bugs y sniffers) conectados al cableado.
- El cableado alrededor de las salas de servidores y centros de datos debería estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.
- Debe tener en cuenta el acceso restringido y controlado a las salas de paneles de conexión.

### 13. Mantenimiento de los equipos

Los equipos deben mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información. Para esto debe tener en cuenta:

- Las recomendaciones del fabricante.
- Que solo personal autorizado debe mantener equipos críticos.
- Mantenga registros de los mantenimientos y de todo lo que considere pertinente.
- La información sensible debería removese del equipo cuando sea necesario.
- Cumplir con todos los requisitos de las pólizas de seguros.

### 14. Eliminación segura o reutilización de equipos

Antes de la eliminación o reutilización, revise y verifique que los equipos que contengan soportes de almacenamiento se han eliminado o sobrescrito de forma segura. Ya sea equipos, software u otros dispositivos de información debe registrar:

- La identificación y autorización de personal autorizado a retirar equipos o activos fuera de la organización.

- Fijar límites de tiempo.
- Documente los equipos retirados y de su retorno, además de la identificación de personal.



# **Anexo 4.**

## **Controles**

## **Tecnológicos**

## Anexo 4. Controles Tecnológicos

En este anexo podrá profundizar sobre los controles tecnológicos del Anexo A de la Norma ISO/IEC 27001.



**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 autorizado, fallas de funcionamientos o por mala administración.

### 1. Dispositivos de punto final de usuario

Se debe establecer un proceso formal para asignar y revocar los accesos a la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario. Para esto:

- Incluya la aprobación del propietario del servicio o sistema.
- Verifique si el acceso cumple con las políticas de acceso definidas.
- Garantice que el acceso no se da hasta finalizar el proceso de autorización.
- Mantenga un registro de los accesos concedidos.
- Elimine los accesos de usuarios que han abandonado la organización.
- Modifique los accesos de usuarios que han cambiado de función o puesto de trabajo si proceda.
- Revise periódicamente los derechos de acceso.

### 2. Derechos de acceso privilegiado

El control y uso de los derechos de acceso privilegiados debe restringirse y gestionarse de forma independiente mediante un proceso específico que:

- Tenga en cuenta las políticas de acceso privilegiado definidas.
- Se identifiquen accesos privilegiados de cada sistema o proceso.
- Se tenga en cuenta las reglas generales de mínimos privilegios.
- Se establezca una norma de caducidad de los permisos privilegiados.
- Se definan IDs especiales o distintos para las cuentas de uso normales o no privilegiadas.
- Se definan procedimientos para evitar el uso no autorizado de cuentas con derechos de acceso privilegiados.
- Se verifiquen periódicamente las competencias de los usuarios.
- Considere mecanismos para mantener la confidencialidad de los datos de acceso de usuarios genéricos para los usuarios privilegiados o mecanismos para forzar el cambio de contraseñas cuando un usuario privilegiado abandona o cambia de puesto de trabajo.

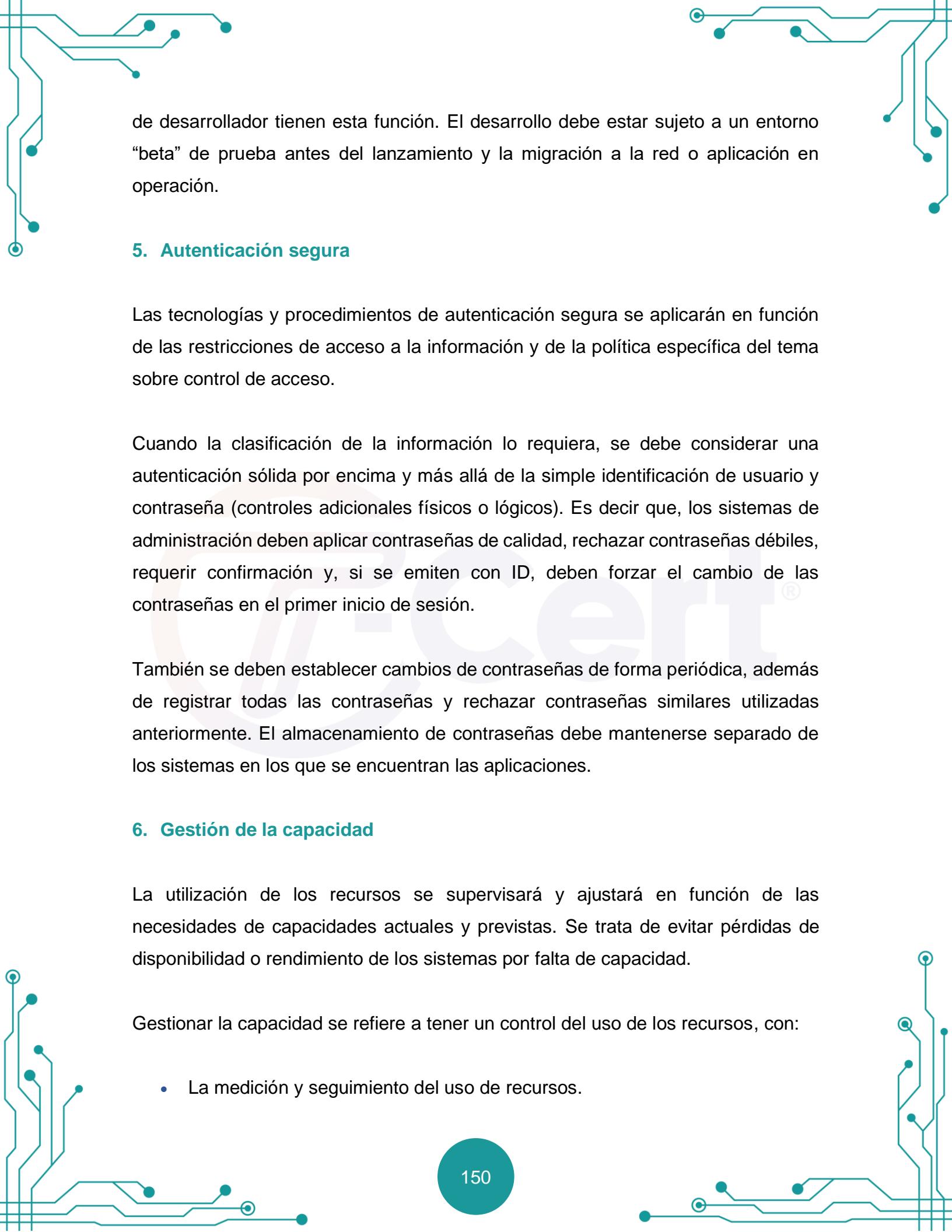
### **3. Restricción del acceso a la información**

El acceso a la información y a otros activos asociados se restringirá de conformidad con la política temática específica establecida en materia de control de acceso. Las funciones de una aplicación o sistema deben considerar las restricciones de control de acceso.

### **4. Acceso al código fuente**

Gestione adecuadamente el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software. El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente. El código fuente no debe protegerse con aplicaciones de red.

Adicionalmente, establezca controles para mantener registros de la salida y de auditoría de los cambios realizados en el código. La mayoría de las herramientas



de desarrollador tienen esta función. El desarrollo debe estar sujeto a un entorno “beta” de prueba antes del lanzamiento y la migración a la red o aplicación en operación.

## 5. Autenticación segura

Las tecnologías y procedimientos de autenticación segura se aplicarán en función de las restricciones de acceso a la información y de la política específica del tema sobre control de acceso.

Cuando la clasificación de la información lo requiera, se debe considerar una autenticación sólida por encima y más allá de la simple identificación de usuario y contraseña (controles adicionales físicos o lógicos). Es decir que, los sistemas de administración deben aplicar contraseñas de calidad, rechazar contraseñas débiles, requerir confirmación y, si se emiten con ID, deben forzar el cambio de las contraseñas en el primer inicio de sesión.

También se deben establecer cambios de contraseñas de forma periódica, además de registrar todas las contraseñas y rechazar contraseñas similares utilizadas anteriormente. El almacenamiento de contraseñas debe mantenerse separado de los sistemas en los que se encuentran las aplicaciones.

## 6. Gestión de la capacidad

La utilización de los recursos se supervisará y ajustará en función de las necesidades de capacidades actuales y previstas. Se trata de evitar pérdidas de disponibilidad o rendimiento de los sistemas por falta de capacidad.

Gestionar la capacidad se refiere a tener un control del uso de los recursos, con:

- La medición y seguimiento del uso de recursos.

- La previsión de uso a futuro (prever “cuellos de botella”).
- La planificación de ampliaciones de capacidad de los recursos cuando sea necesario
- La optimización del uso de recursos.

## 7. Protección contra malware

Garantice la protección contra programas maliciosos, también aplique y apóyese en la concienciación adecuada de los usuarios. En primer lugar, disponga de sistemas de detección de código malicioso en los servidores y en los puestos de trabajo.

- La primera línea de defensa para evitar la entrada de código malicioso son los propios usuarios, que deben estar preparados para saber responder ante posibles incidencias detectadas.
- La segunda línea de defensa debe enfocarse al acceso a los sistemas para restringir cómo los usuarios conectan medios extraíbles u otros dispositivos a las redes para evitar la introducción de material no verificado.

Algunos requisitos para abordar la detección de malware son:

- Definir responsabilidades sobre los que tienen la misión específica de realizar las tareas detección de malware y las de los usuarios.
- Realizar las capacitaciones necesarias para que el personal dedicado a la tarea de detección de Software malicioso tenga los conocimientos necesarios.
- Capacitar a los usuarios para que sepan cómo deben actuar cuando reciben una alarma de detección de software malicioso.
- Establecer procedimientos para las tareas de mantenimiento y las situaciones de emergencia.
- Establecer procedimientos de aislamiento en caso de detección y recuperación de cualquier ataque.

- Incluir en las políticas de seguridad las acciones y procedimientos establecidos en los planes de continuidad del negocio para casos de recuperación ante incidentes.

## 8. Gestión de vulnerabilidades técnicas

Obtenga información sobre las vulnerabilidades técnicas de los sistemas de información en uso, después evalúe la exposición de la organización a dichas vulnerabilidades para tomar las medidas adecuadas. Para esto, identifique las posibles debilidades técnicas mediante:

- La consulta de foros especializados.
- Mantener actualizada la información de fabricantes y proveedores.
- Realizar pruebas de ataques simulados (hacking ético).
- Escaneos periódicos de vulnerabilidades.

## 9. Gestión de la configuración

Establezca, documente aplique, supervise y revise las configuraciones, incluidas las configuraciones de seguridad, del hardware, el software, los servicios y las redes.

## 10. Eliminación de información

La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.

## 11. Enmascaramiento de datos

El enmascaramiento de datos se utilizará de acuerdo con la política específica de la organización en materia de control de acceso y otras políticas específicas

relacionadas, así como con los requisitos de la empresa, teniendo en cuenta la legislación aplicable.

## 12. Prevención de fugas de datos

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

## 13. Copia de seguridad de la información

Las copias de seguridad de la información, los programas informáticos y los sistemas se mantendrán y comprobarán periódicamente de acuerdo con la política específica acordada en materia de copias de seguridad. Evite la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.

Tenga en cuenta:

- **Alcance de las copias de seguridad:** Asegúrese que las copias de seguridad tienen un alcance que cubra todas las necesidades de respaldo de su información, como:
  - Datos e información sensible.
  - Software y aplicaciones.
  - Datos de configuración de aplicaciones Sistemas etc.
  - Datos sobre accesos, claves etc.
  - Registros de actividades, eventos, mensajes o alarmas del sistema.
- **Verifique su validez:** Compruebe que las copias son válidas.
- **Ubicaciones Alternativas:** No solo es importante realizar las copias de seguridad sino la ubicación donde se encuentran. Puede establecer ubicaciones alternativas al emplazamiento de los datos o aplicaciones para

aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios etc.

- **Medios de recuperación:** Los medios de recuperación son tan importantes como las propias copias de seguridad, por lo que debe tener en cuenta el mantenimiento en perfecto estado de funcionamiento de los medios que permitirán la restauración de las copias cuando se necesiten.
- **Restauraciones parciales:** Los medios de recuperación y el sistema de copias de seguridad, deben permitir restauraciones parciales del sistema dependiendo de las distintas aplicaciones y sistemas de forma que un incidente de corrupción de un sistema o aplicación no obligue a la restauración de otras aplicaciones con el consiguiente impacto.
- **Mantener registros:** Mantenga registros de las copias de seguridad como parte de un cronograma o plan de mantenimiento de copias de seguridad. También es aconsejable mantener un registro de las pruebas de validez de dichas copias.
- **Nivel de protección:** Mantenga el mismo nivel de protección para las copias de seguridad que los requeridos para los datos operativos y cuando sea necesario las copias de seguridad deben estar encriptadas.

## 14. Redundancia de las instalaciones de tratamiento de la información

Las instalaciones de procesamiento de la información se deben implementar con la redundancia suficiente para cumplir los requisitos de disponibilidad.

## 15. Registro

Se deben crear, almacenar, proteger y analizar los registros que recojan actividades, excepciones, fallos y otros eventos relevantes. De esta forma se podrá determinar qué estaba sucediendo mediante los datos de la hora, la fecha del incidente, etc., las personas involucradas, el origen y las causas, etc.

La primera tarea será determinar los distintos eventos a registrar en cada sistema:

- Intentos de acceso exitosos y fallidos.
- Desconexiones del sistema.
- Acciones ejecutadas.
- Alertas por fallos en el sistema.
- Fecha y hora en que se producen los eventos.
- Tiempos de detención, etc.

Adicionalmente, tenga en cuenta:

- **Los aspectos legales:** Tener un sistema sin un registro de eventos puede ser un grave error ya que en algunos casos puede implicar sanciones por incumplimiento de las normas legales sobre protección de datos personales.
- **Prevenir incidentes:** Revisar los registros de forma periódica, independientemente de si hay un incidente o no puede ayudar en el análisis de tendencias, detectar actividades fraudulentas potenciales, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes.

## 16. Seguimiento de las actividades

Supervise las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se adopte las medidas adecuadas para evaluar posibles incidentes relacionados con la seguridad de la información. Para esto:

- Los registros de eventos deben tener el nivel de protección apropiado para evitar pérdidas, corrupción o cambios no autorizados.
- El administrador del sistema no debe tener permiso para borrar o desactivar el registro de sus propias actividades.
- Guarde copias de seguridad de los registros de eventos.

- La detección de intrusiones debe ser administrada fuera del alcance de los administradores de red.

## 17. Sincronización de relojes

Los relojes de los sistemas de tratamiento de la información utilizados por la organización deberán estar sincronizados con las fuentes horarias aprobadas.

Aunque existan otros requisitos de sincronización en el sistema, a la hora de registrar eventos es imprescindible que todos los sistemas de procesamiento estén sincronizados. Para cumplir con este requisito, el proceso de sincronización debe estar documentado con los requisitos necesarios para que esto se cumpla.

## 18. Uso de programas de utilidades privilegiadas

El uso de programas de utilidades que puedan ser capaces de anular los controles del sistema y de las aplicaciones deberá estar restringido y estrictamente controlado.

## 19. Instalación de software en sistemas operativos

Es importante aplicar procedimientos y medidas para gestionar de forma segura las instalaciones de software en los sistemas operativos. Para esto:

- Pruebe las nuevas aplicaciones o software en entornos aislados especialmente preparados para pruebas.
- Compruebe las necesidades de instalación (compatibilidad del entorno) antes de su instalación.
- Valorar la necesidad de actualización o instalación.
- Planifique la forma de volver a versiones anteriores en caso de ser necesario.

- Asegúrese de que los entornos de desarrollo permanezcan aislados de los entornos operativos.
- Las instalaciones de software sean realizadas por usuarios autorizados.
- Establezca procedimientos o herramientas de monitoreo del software para detectar cambios no autorizados.
- Supervise las pruebas posteriores a la implementación de la red para identificar cualquier tráfico inesperado que pueda exponer errores o suponga empeoramiento de la velocidad de las transmisiones.

## 20. Seguridad de las redes

Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información de los sistemas y aplicaciones. Considere la posibilidad de separar el control de la red de las tareas de operación.

Los principales elementos a gestionar dentro de una red son los elementos físicos que dan soporte a la red y sobre todo los que interconectan a la organización con el exterior (routers, switch, etc.).

Cuando la información se transfiere a través de redes públicas o redes inalámbricas, se deben considerar controles adicionales para mantener las conexiones (disponibilidad), la privacidad (confidencialidad) y la integridad de los datos. Para esto:

- **Monitoree y registre:** El monitoreo y registro de las actividades en la red se deben utilizar para establecer medidas correctivas y si es necesario disciplinarias, así como también para establecer medidas preventivas.
- **Controle el acceso:** La autenticación de inicio de sesión para el uso de la red puede ser implementada mediante un sistema de garantía de factores múltiples.

- **Controle los privilegios:** Como control fundamental de cualquier sistema las conexiones de red también deben estar restringidas según los privilegios asignados.

## 21. Seguridad de los servicios de red

Independientemente de si los servicios de red son internos o externos (subcontratados), deben definirse, aplicarse y supervisarse requisitos en relación a la calidad de servicio mediante acuerdos de Niveles de Servicio o SLA.

Las auditorías de la calidad de servicios prestados, es el único modo en que se tiene visibilidad sobre la disponibilidad de la red y la evaluación de los riesgos a los que se expone la organización con dichos servicios, ya que de ellos depende la operatividad de los sistemas de información.

## 22. Segregación de redes

Los grupos de servicios de información, usuarios y sistemas de información deberán estar segregados en las redes de la organización. La segregación o separación de redes puede aplicarse de forma lógica o incluso física.

## 23. Filtrado web

El acceso a sitios web externos se gestionará para reducir la exposición a contenidos maliciosos.

## 24. Uso de la criptografía

Defina y aplique normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas. Los controles criptográficos están enfocados en la protección de la información en el caso de que un intruso pueda tener acceso físico a la

información, se impone establecer un sistema de cifrado de la misma para dificultar la violación de su confidencialidad o su integridad.

En una política de implementación y administración de claves de cifrado de datos se debe identificar a un responsable de la política para su implementación y administración. La clave de la política de controles criptográficos está en identificar:

- Para que información y en qué circunstancias será necesario aplicar claves criptográficas.
- Los medios a emplear.
- La gestión, mantenimiento y actualización de dichos medios.

## 25. Ciclo de vida del desarrollo seguro

Cree y aplique normas para el desarrollo seguro de software y sistemas. La evaluación de riesgos para la seguridad de la información no solo debe afectar a los activos de información como software, datos o equipos y soportes, sino que también debe aplicarse a los entornos de desarrollo, los procesos de desarrollo y las tecnologías utilizadas para determinar si es necesario aplicar medidas o controles de seguridad. Debe tener en cuenta:

- El grado de sensibilidad de los datos.
- Los niveles de seguridad aplicables.
- Los controles de seguridad definidos para cada tipo de información.
- La confiabilidad del personal.
- Las necesidades de separar entornos de desarrollo.
- Los controles de acceso determinados para el entorno de desarrollo.
- Las necesidades de respaldo de información.
- Los controles y políticas para el traslado de información.

## **26. Requisitos de seguridad de las aplicaciones**

Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse cuando se desarrollen o adquieran aplicaciones.

## **27. Arquitectura de sistemas seguros y principios de ingeniería**

Forme, documente, mantenga y aplique principios de ingeniería de sistemas seguros a todas las actividades de desarrollo de sistemas de información.

## **28. Codificación segura**

Aplique principios de codificación segura al desarrollo de software.

## **29. Pruebas de seguridad en el desarrollo y la aceptación**

Los procesos de pruebas de seguridad se definirán y aplicarán en el ciclo de vida del desarrollo. Los requisitos para la seguridad de un sistema software deben ser probados como si se tratase de una funcionalidad más del software. Para ello debe implementar un plan de pruebas documentado. Las pruebas también deben incluirse al software subcontratado.

El proceso de incorporación de nuevas aplicaciones actualizaciones o nuevas versiones de software debe estar sujeto a un proceso de aceptación donde se le realicen las pruebas funcionales y de seguridad planificadas. Los entornos de pruebas deben ser distintos a los entornos de operación para evitar fallos en sistemas reales.

### **30. Desarrollo subcontratado**

La organización debe dirigir, supervisar y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.

Para la subcontratación de desarrollos de Software debe tener en cuenta:

- Establecer y supervisar el cumplimiento de los requisitos de seguridad.
- Controlar y gestionar todos los aspectos de licencias y propiedades de código fuente.
- La metodología y definición de las pruebas a realizar al software subcontratado.
- Todo lo anterior debe ser plasmado en acuerdos firmados y consensuados con el proveedor.

### **31. Separación de los entornos de desarrollo, prueba y producción**

Los entornos de desarrollo, pruebas y producción deben estar separados y protegidos, para evitar problemas de indisponibilidad o fallos en el servicio.

### **32. Gestión del cambio**

Los cambios en las instalaciones de tratamiento de la información y en los sistemas de información estarán sujetos a procedimientos de gestión de cambios. Los procesos de cambio pueden conllevar riesgos asociados para la seguridad de la información. Es necesario analizar los procesos de cambio:

- Comerciales.
- Instalaciones o infraestructuras (Equipos y Software).
- Sistemas de procesamiento de información.

Adicionalmente, mantenga un registro que contenga al menos la información de:

- Quien autoriza los cambios.
- Quien realiza los cambios.
- Fecha.
- Descripción de las tareas.
- Validación del cambio.
- Otros.

Esta información será útil en una auditoría para proporcionar la confianza de que los cambios se han realizado de forma controlada.

### **33. Información de la prueba**

La información de las pruebas debe ser seleccionada, protegida y gestionada de forma adecuada.

### **34. Protección de los sistemas de información durante las pruebas de auditoría**

Las pruebas de auditoría y otras actividades de garantía que impliquen la evaluación de los sistemas operativos se planificarán y acordarán entre la persona encargada de las pruebas y la dirección correspondiente.

# 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 Combinada:** Auditoría llevada a cabo conjuntamente a un único auditado en dos o más sistemas de gestión.

**Auditoría Conjunta:** Auditoría llevada a cabo a un único auditado por dos o más organizaciones auditadoras.

**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.

**Conclusiones de la Auditoría:** Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

**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.

**Evidencia de la Auditoría:** Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que es verificable.

**Evidencia Objetiva:** Datos que respaldan la existencia o veracidad de algo.

**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.

**Hallazgos de la Auditoría:** Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

**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:** 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.

**Plan de Auditoría:** Descripción de las actividades y de los detalles acordados de una auditoría.

**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.

**Programa de Auditoría:** Acuerdos para un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

**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. 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 en 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.