



fcfm

ESCUELA DE POSTGRADO
Y EDUCACIÓN CONTINUA
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

ISO 27001:2022

Interpretación de Requisitos

Fundamentación

La implementación de modelos de gestión basados en ISO 27001 se ha convertido en un proceso fundamental para las organizaciones para **mejorar la seguridad de la información y la eficacia en el logro de sus metas**, de manera de aplicar herramientas y prácticas que les permitan enfrentar nuevos desafíos en los diferentes ámbitos de la industria en la que se desempeñen.

Objetivo general

- Comprender y adquirir los conocimientos de la norma ISO 27001:2022, de manera tal que, al finalizar el programa, los participantes sean capaces de comprender la norma con sus componentes y saber aplicar los requisitos normativos de ésta en su propia organización.

Contenidos

1. Cambios respecto de la versión anterior.
2. Introducción al Sistema de Gestión de Seguridad de la Información ISO/IEC 27001:2022
3. Referencias normativas de la Familia de normas de ISO 27001
4. Interpretación de requisitos de ISO/IEC 27001:2022 en el contexto de los Sistemas de Gestión de Seguridad de la Información

Cambios introducidos en ISO/IEC 27001:2022 respecto de su versión anterior



ISO/IEC 27001:2022



El mundo actual es muy diferente al de 2013...

- Pasamos por una pandemia de SARS CoV-2 con el impacto cultural, económico y tecnológico desde el 2019 hasta la fecha.
- El confinamiento hizo que las organizaciones maximizasen el uso de recursos y optar por el teletrabajo, educación a distancia e interacción de los equipos de trabajo por medio de herramientas de trabajo colaborativo.
- Incremento del acceso a Internet por medio de dispositivos móviles (estamos ad portas del 5G generalizado en el mundo móvil).
- Cambio en el paradigma de los DATACENTERS dando un gran impulso a consumir servicios desde la nube.
- Incremento de ciberataques a distintas organizaciones en todo el mundo durante la pandemia.
- Aparición de nuevos tipos de malware como es el RAMSOMWARE (ej.: WanaCrypt0r).

ISO/IEC 27001:2022



El mundo actual es muy diferente al de 2013...

- Nueva normativa relativa a protección de los datos personales, siendo el Reglamento General de Protección de Datos (RGPD), que entró en vigor en mayo de 2016 y fue de aplicación el 25-05-2018 en la Unión Europea.
- Surgimiento de nuevos activos tecnológicos para impulsar el Internet de las cosas (IoT).
- Generación de un gran volumen de información cada segundo desde los millones de dispositivos que se conectan a internet.
- ...

Cambios respecto de la versión anterior

El título

El nombre se ha cambiado para reflejar el alcance real de la norma. Ahora es **ISO/IEC 27001:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.**

Esto también se alinea con el nuevo título de **ISO/IEC 27002:2022** (Seguridad de información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información).

Cambios respecto de la versión anterior

Numeración de cláusulas

Se ha introducido nuevas subcláusulas para armonizar aún más la estructura del documento con otras normas de sistemas de gestión, como ISO 9001 e ISO 22301.

También se intercambiaron dos subcláusulas, 10.1 y 10.2. Ahora 10.1 es Mejora Continua mientras que 10.2 es No Conformidad y Acción Correctiva. No hay cambios en sus requisitos.

Cambios respecto de la versión anterior

Nuevo texto

Aunque se ha agregado texto nuevo y se ha reorganizado algo, estos cambios solo aclaran los requisitos y no agregan otros nuevos a la norma (texto introducido en las cláusulas 4.2, 4.4, 5.1, 5.3, 6.2, **6.3**, 7.4, 8.1, 9.1, 9.3.2)

Pero...

Cambios respecto de la versión anterior

Sin profundizar en los detalles, los impactos son:

Cláusula 4

Identificar el contexto interno y el entorno de la organización. La nueva norma, al abarcar el ciberespacio involucra analizar el entorno a una mayor profundidad y sus implicaciones.

Identificar las partes interesadas: Grupos que estarán preocupados ahora por la privacidad y la ciberseguridad. Entonces en forma automática el alcance del Sistema de Gestión cambia.

Cláusula 5

En esta cláusula identificamos la política de seguridad de la información que obviamente deberá ampliarse para ser Política de seguridad de la información, ciberseguridad y protección de la privacidad.

Cláusula 6

Planificación: la gestión de riesgos debe ampliarse al considerar no sólo los activos de la organización, sino también los activos personales, y los activos del ciberespacio.

Cambios respecto de la versión anterior

Cláusula 7

Aparentemente no existen cambios en su contenido, pero al considerar los recursos para cubrir privacidad y ciberseguridad, el cambio se experimentará al implementarse.

Cláusula 8

El tratamiento de riesgos y el uso del anexo A y en consecuencia la norma ISO 27002 implica un desafío para entender y aplicar el nuevo esquema de controles u homologar con los controles existentes.

Cláusula 9

La evaluación deberá considerar el alcance definido en la cláusula 4, igualmente el monitoreo de los controles de forma consistente a lo largo del tiempo va a afectar la implementación y cumplimiento de esta cláusula.

Cláusula 10

La mejora ya no sólo provendrá desde el interior de la organización, cambios reglamentarios, en el entorno, cambios tecnológicos en el ciberespacio, también son fuentes que deberán de considerarse para la mejora y adaptación del sistema de gestión.

Cambios respecto de la versión anterior

Anexo A

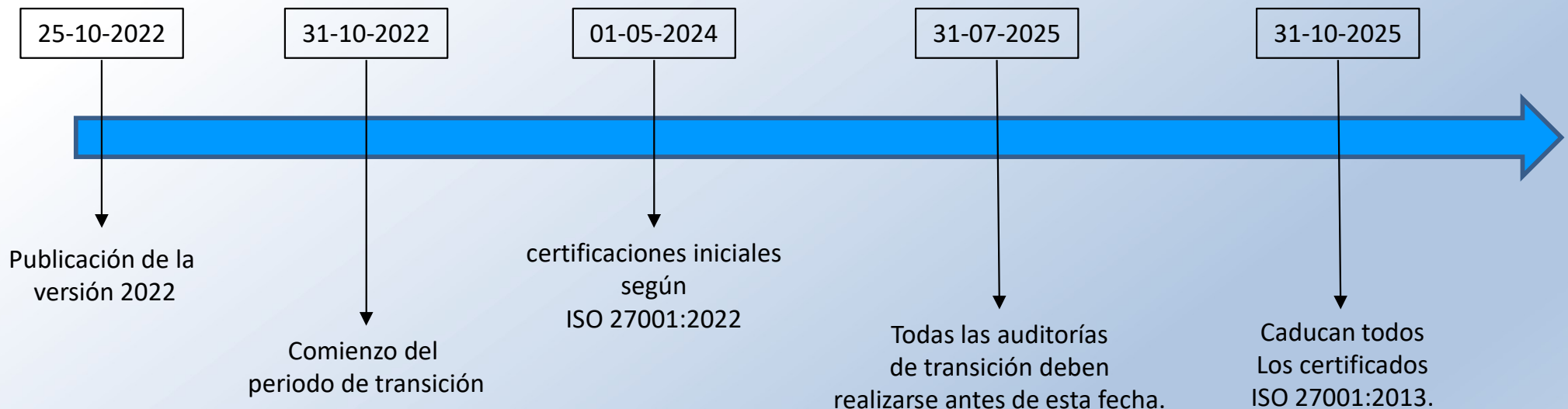
El título del Anexo A ahora es **Referencia de controles de seguridad de la información** y los controles se han revisado para alinearse con ISO/IEC 27002:2022. En la edición de 2013, solo las descripciones de los controles se derivan de ISO/IEC 27002.

Reducción de 114 a 93 controles en 4 categorías de control

Los controles se reagrupan en 4 categorías, en lugar de 14 temas y 35 categorías en la edición 2013.

¿Cuánto durará el período de transición?

El período de transición será de tres años a partir de la publicación oficial de ISO/IEC 27001:2022, esto es a partir del:



Introducción al Sistema de Gestión de Seguridad de la Información (SGSI) ISO/IEC 27001:2022





Introducción al SGSI ISO/IEC 27001:2022

Las organizaciones de todo tipo y tamaño:

- a) recopilan, procesan, almacenan y transmiten información;
- b) reconocen que la información, el entorno, la regulación aplicable, los procesos, los sistemas, las redes y las personas relacionadas son activos importantes para lograr los objetivos de la organización;
- c) enfrentan una gama de riesgos que pueden afectar el funcionamiento de los activos; y
- d) abordan su exposición al riesgo percibida mediante la implementación de controles de seguridad de la información.

Introducción al SGSI ISO/IEC 27001:2022

Toda la información mantenida, conservada y procesada por una organización está sujeta a:

- amenazas de ataque,
- a errores,
- a eventos de la naturaleza (inundación, incendio, etc.), y está sujeto a vulnerabilidades inherentes a su uso.

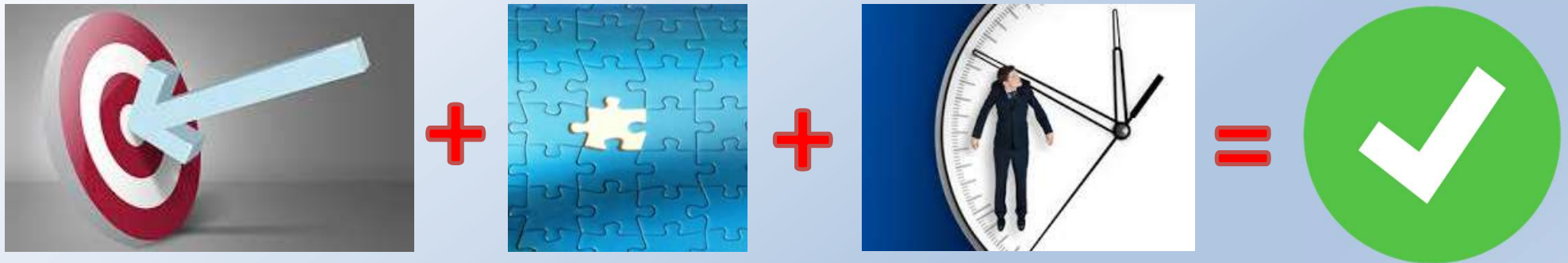
Introducción al SGSI ISO/IEC 27001:2022

- La seguridad de la información usualmente se basa en la información considerada como un activo que tiene un valor que requiere una protección adecuada (ej.: contra la pérdida de disponibilidad, de confidencialidad y de integridad).



Introducción al SGSI ISO/IEC 27001:2022

- Permitir que la información exacta y completa esté oportunamente disponible para aquellos con una necesidad autorizada es un estimulante para el desarrollo de la eficiencia empresarial.





Introducción al SGSI ISO/IEC 27001:2022

- El sistema de gestión de la seguridad de la información SGSI conserva la **confidencialidad**, **integridad** y **disponibilidad** de la información al aplicar un proceso de **gestión de riesgo** y le entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada.

Introducción al SGSI ISO/IEC 27001:2022

- El SGSI debe formar parte y estar **integrado a los procesos de la organización** y a la estructura de gestión general.
- La seguridad de la información debe ser **considerada en el diseño de sus procesos, de sus sistemas de información y de sus controles.**



Qué es un SGSI

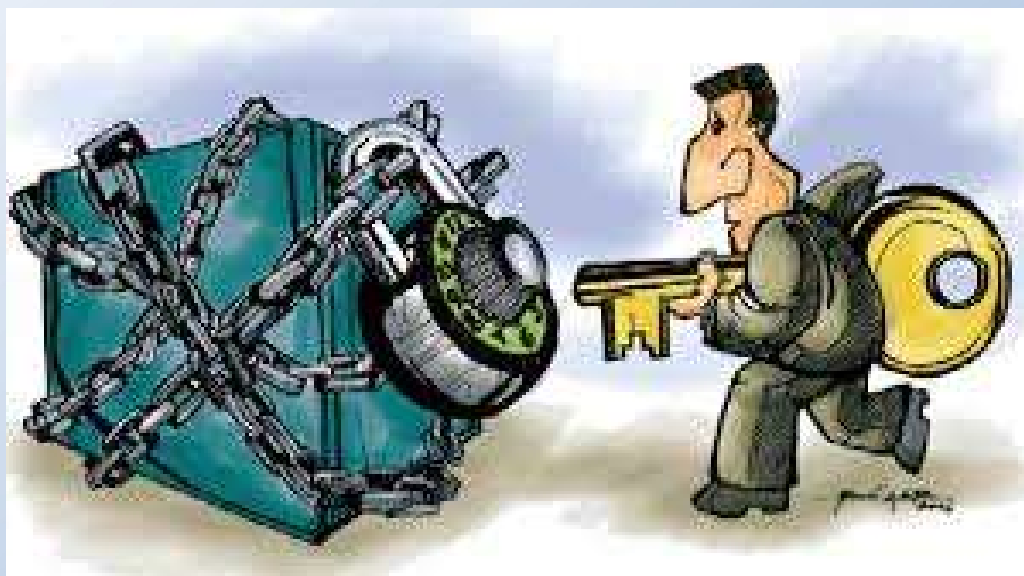
SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información.



Qué es un SGSI



Información: Es **toda la documentación en poder de una organización**, independiente de la forma en que se guarde, contenga o transmita, de su origen y de su fecha de elaboración.



- **Confidencialidad:** La información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
- **Integridad:** La información es precisa y completa.
- **Disponibilidad:** La información debe ser accesible y utilizable a pedido por una entidad autorizada.

Fuente: ISO 27000:2018

- **Ciberseguridad:** Condición de estar protegido contra consecuencias físicas, sociales, espirituales, financieras, políticas, emocionales, ocupacionales, psicológicas, educativas o de otro tipo de fallas, daños, errores, accidentes o cualquier otro evento en el Ciberespacio que pueda considerarse no deseable.
- **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet por medio de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física.

(Fuente: ISO 27032)

- **Protección de la privacidad:** Es estar libre de intrusiones o perturbaciones en la vida privada o en los asuntos personales.

(Fuente: CEPAL)

En el ámbito de ISO 27001 ello está relacionado solo con el manejo de la información personal

La **seguridad de la información** consiste en la **preservación** de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.



Una **falla de seguridad** es cualquier incidente que compromete o que pone en peligro cualquiera de los aspectos con los que se valora la seguridad de la información.



Con la actual complejidad de los sistemas de información es fácil hacerse una idea del reto que presenta evitar que sucedan cosas como:

- Fallas en las comunicaciones.
- Fallas en el suministro eléctrico.
- Fallas humanas de usuarios internos, usuarios externos, administradores, programadores, etc.
- Fallas en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc. que inundan la red.
- Accesos no autorizados a los sistemas o a la información.
- Incumplimiento de una ley o un reglamento.
- ...

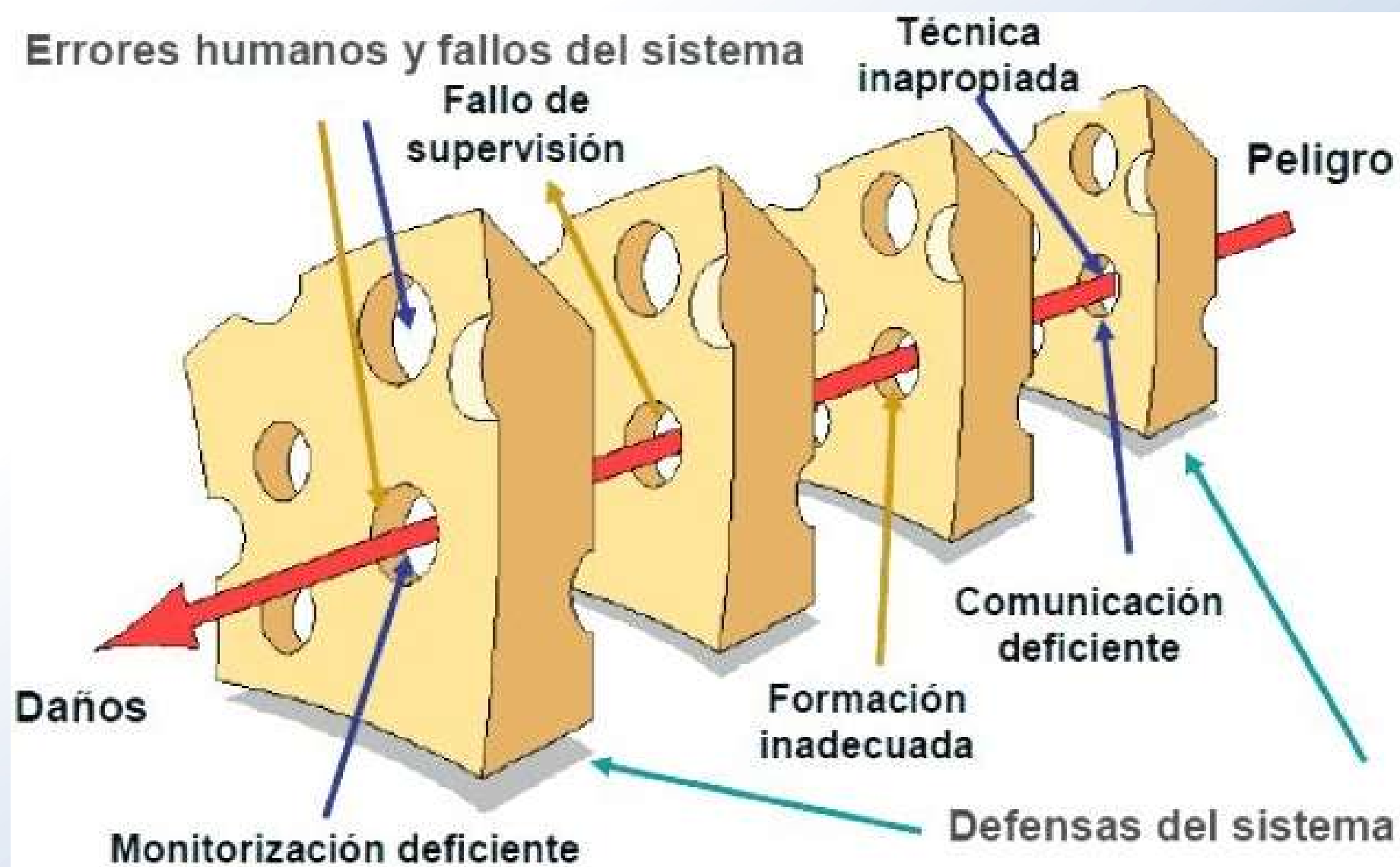
Las fallas de seguridad son ocasionadas, muchas veces, por la **errónea percepción** de que, si la seguridad física está asegurada, no tiene por qué haber problemas; o que protegiendo únicamente las aplicaciones y las bases de datos ya está garantizada la seguridad.

Estos supuestos dejan desprotegidas áreas de la organización.

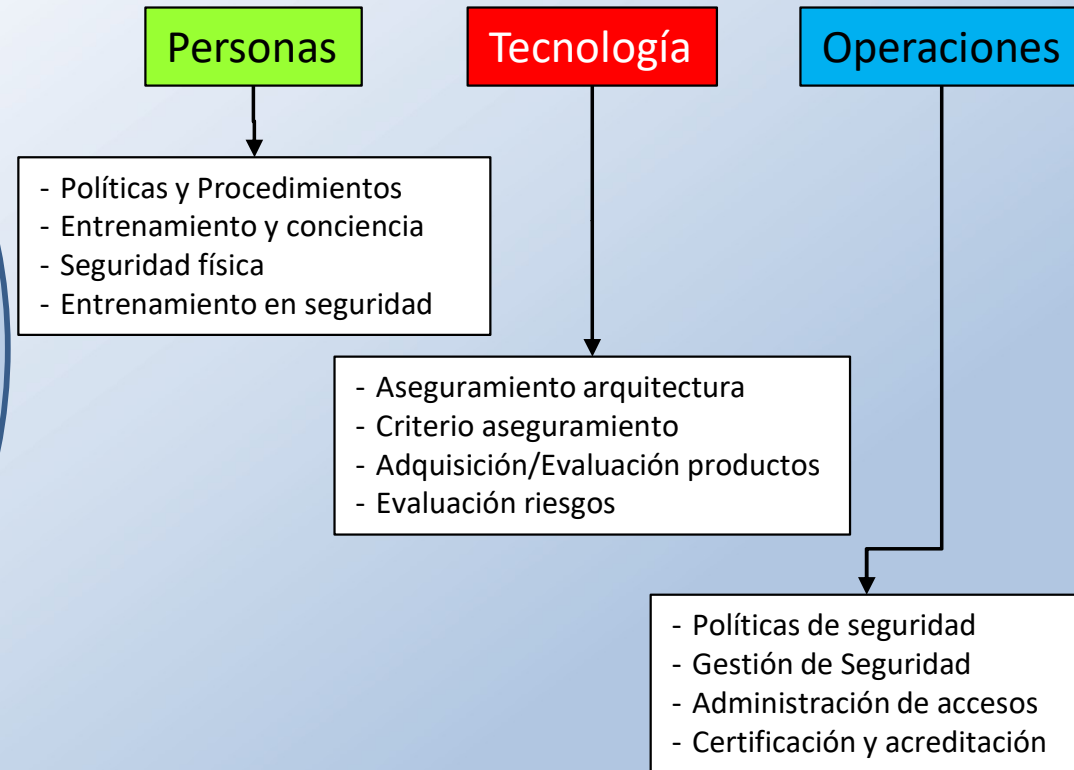
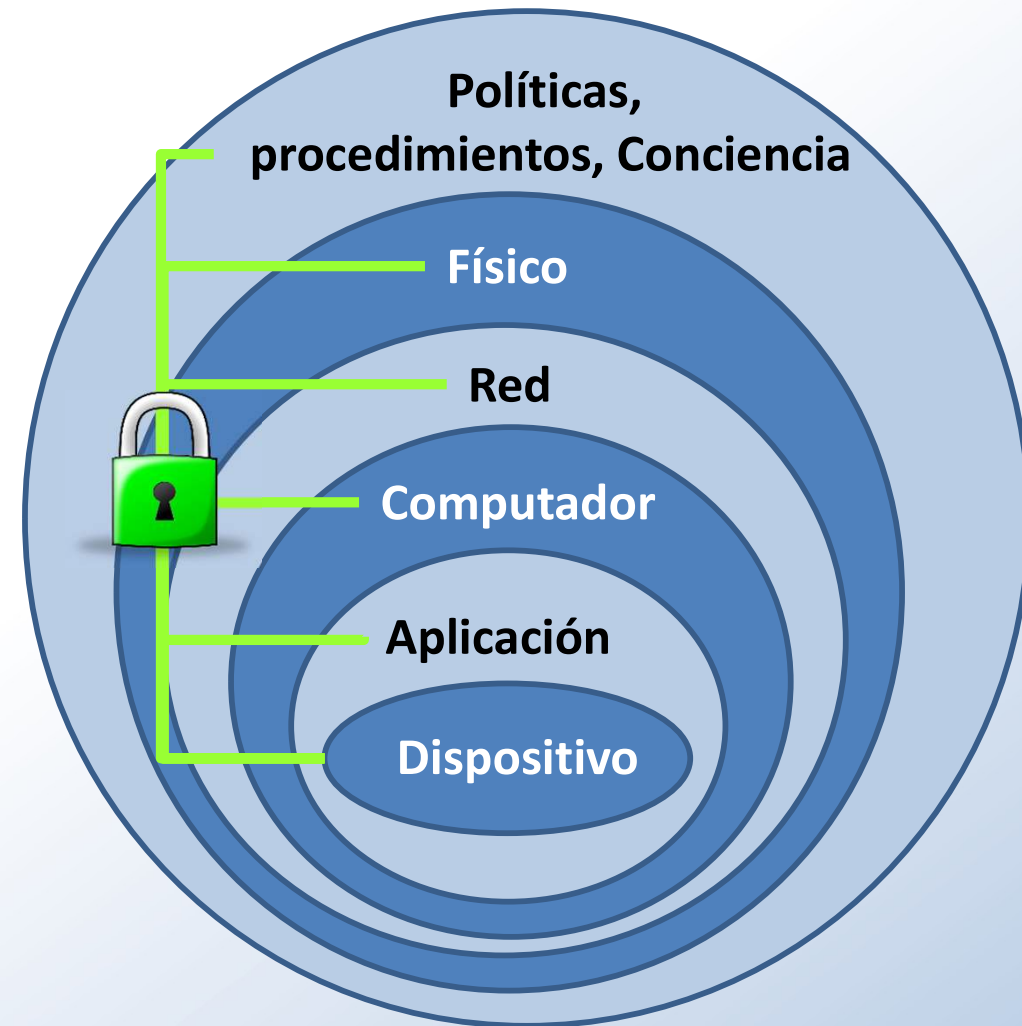
Los activos de información pueden ser fácilmente dañados o destruidos, ya que no se ha tenido en cuenta todos los aspectos de la seguridad de la información: **la seguridad física, la seguridad lógica y las medidas organizativas.**



**Activos de
Información**



Estrategia de Defensa en Profundidad



La seguridad de la Información...

- Se logra mediante la implementación de:

un conjunto adecuado de controles, incluidas políticas, reglas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware.

3 fuentes principales de requisitos de SI

- Evaluación de riesgos para la organización, teniendo en cuenta la estrategia y objetivos empresariales generales de la organización. Esto se puede facilitar o apoyar a través de una evaluación de riesgos específica para seguridad de la información. Esto debería dar lugar a la determinación de controles necesarios para garantizar que el riesgo residual para la organización cumple con sus criterios de aceptación del riesgo;
- Requisitos legales, reglamentarios y contractuales que deberían cumplir una organización y sus partes interesadas (socios comerciales, proveedores de servicios, otros) y su entorno sociocultural;
- Conjunto de principios, objetivos y requisitos empresariales para todas las etapas del ciclo de vida de información que una organización desarrolló para apoyar sus operaciones.

Entonces, un SGSI...

- Consiste en políticas, procedimientos, directrices, recursos y actividades asociadas, administrados colectivamente por una organización, en busca de **proteger sus activos de información**.
- Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para **lograr sus objetivos de negocio**.
- Se basa en una **evaluación de riesgos** y en los niveles de aceptación de riesgos de la organización diseñados para **tratar y administrar los riesgos de manera efectiva**.

Estructura de ISO/IEC 27001:2022

- 10 cláusulas con 58 “debe”
- Anexo A con 4 objetivos de control y 93 controles establecidos.
- **Exclusiones no permitidas** en las cláusulas 4 a 10 de la norma, excepto para los controles del Anexo A.





Referencia de controles de seguridad de la información (Anexo A)

- Controles organizativos = 37
- Controles de personas = 8
- Controles físicos = 14
- Controles tecnológicos = 34



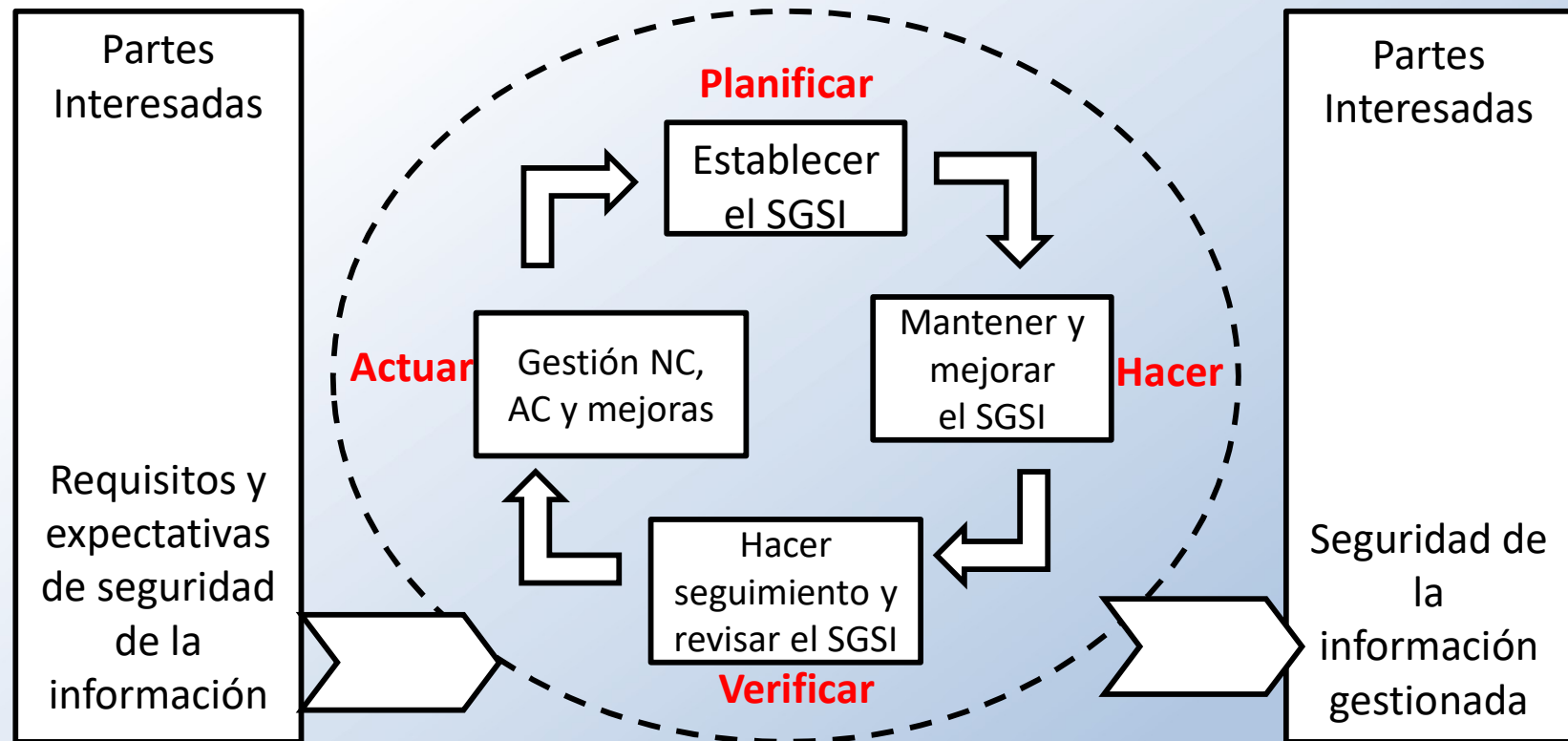
Total = 93 controles en 4 ámbitos

Un control se define como una **medida que elimina, modifica o mantiene el riesgo.**

La norma ISO 27002:2022 proporciona una mezcla genérica de controles de seguridad de la información organizativos, humanos, físicos y tecnológicos derivados de las mejores prácticas reconocidas internacionalmente.

- Si bien el número de controles disminuye, en la práctica no se ha eliminado ninguno, además aparecen 11 nuevos:
 - Inteligencia de amenazas.
 - Seguridad de la información para servicios en la nube.
 - Preparación de las TI para continuidad del negocio.
 - Monitoreo y supervisión de la seguridad física.
 - Gestión de configuración.
 - Eliminación de la información.
 - Enmascaramiento de datos.
 - Prevención de fuga de datos.
 - Actividades de seguimiento.
 - Filtrado web.
 - Codificación segura.

PHVA aplicado a ISO 27001



Referencias normativas de la familia ISO 27001



Normas de la familia 27001 (1/4)

21 normas conforman la familia ISO 27001

- ISO/IEC 27000, Tecnología de la información – Técnicas de seguridad - Seguridad de la información - sistemas de gestión - Descripción general y vocabulario
- **ISO/IEC 27001**, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos
- ISO/IEC 27002, Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información
- ISO/IEC 27003, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Orientación
- ISO/IEC 27004, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación
- ISO/IEC 27005, Tecnología de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información

Normas de la familia 27001 (2/4)

- **ISO/IEC 27006**, Tecnología de la información - Técnicas de seguridad - Requisitos para organismos que realizan auditorías y certificación de sistemas de gestión de seguridad de la información
- ISO/IEC 27007, Tecnología de la información - Técnicas de seguridad - Directrices para la auditoría de sistemas de gestión de seguridad de la información
- ISO/IEC TR 27008, Tecnología de la información - Técnicas de seguridad - Directrices para auditores sobre controles de seguridad de la información
- **ISO/IEC 27009**, Tecnología de la información - Técnicas de seguridad - Aplicación sectorial específica de ISO/IEC 27001 - Requisitos
- ISO/IEC 27010, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información para comunicaciones intersectoriales e interorganizacionales

Normas de la familia 27001 (3/4)

- ISO/IEC 27011, Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información basados en ISO/IEC 27002 para organizaciones de telecomunicaciones
- ISO/IEC 27013, Tecnología de la información - Técnicas de seguridad - Orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1
- ISO/IEC 27014, Tecnología de la información - Técnicas de seguridad - Gobernanza de la seguridad de la información
- ISO/IEC TR 27016, Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Economía de la organización
- ISO/IEC 27017, Tecnología de la información - Técnicas de seguridad - Códigos de práctica para controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube

Normas de la familia 27001 (4/4)

- ISO/IEC 27018, Tecnología de la información - Técnicas de seguridad - Códigos de práctica para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores PII
- ISO/IEC 27019, Tecnología de la información - Técnicas de seguridad - Controles de seguridad de la información para la industria de servicios de energía
- **ISO/IEC 27021**, Tecnología de la información - Técnicas de seguridad - Requisitos de competencia para profesionales de sistemas de gestión de seguridad de la información
- ISO 27799, Informática de la salud: gestión de la seguridad de la información en salud utilizando ISO/IEC 27002
- Guía ISO 73: 2009, Gestión de riesgos - Vocabulario

Legislación chilena relacionada

Constitución Política de la República

- Artículos 8, 19, 24, 39, ...

Código Procesal Penal

Código Penal

Código de Justicia Militar

Ley N°19.913

Ley N°19.974

Ley N° 21459

(derogó la Ley 19.223)

Ley N° 20.009

Ley N° 18.168

Ley N°20.453

Ley N°19.799

Ley N°20.285

Ley N°19.628

Ciberseguridad

D.S. N°83/2005

D.S. N°1.299/2004

D.S. N°1/2015

D.S. N°533/2015

Fuente: Política Nacional de Ciberseguridad
<https://www.ciberseguridad.gob.cl/>

Interpretación de requisitos de ISO/IEC 27001:2022 en el contexto de los Sistemas de Gestión de Seguridad de la Información



Nota: El texto utilizado en este documento corresponde a la norma UNE-ISO/IEC 27001:2023 correspondiente a ISO/IEC 27001:2022

Capítulos Introductorios:

1. Alcance y campo de aplicación.
2. Referencias normativas.
3. Términos y definiciones

Importante: Estos capítulos **no constituyen requisitos auditables**

1. Alcance y campo de aplicación (extracto).

Define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de la organización.

Incluye los requisitos para la evaluación y tratamiento de los riesgos de la seguridad de la información adaptados a las necesidades de la organización.

2. Referencias normativas (extracto).

La versión 2022 de ISO 27001 solo hace referencia a las normas siguientes:

- ISO/IEC 27000, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

3 Términos y definiciones

Para los propósitos de esta norma, se aplican los términos y definiciones proporcionados en ISO/IEC 27000.



Capítulos de Requisitos:

4. Contexto de la organización.

5. Liderazgo.

6. Planificación.

7. Apoyo.

8. Operación.

9. Evaluación de desempeño

10. Mejora

4. Contexto de la organización

4.1 Comprender la organización y su contexto:

La organización **debe** determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información..

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

(fuente: ISO/IEC 27000:2018)

4. Contexto de la organización

4.1 Comprender la organización y su contexto...



La organización y su contexto

Establecer las cuestiones externas e internas a la organización que pueden **afectar al propósito de la misma y su dirección estratégica**, y que por tanto deben tenerse en cuenta en el SGSI.



La organización y su contexto

Externo a nivel internacional, nacional, regional o local	<ul style="list-style-type: none">• Cultural• Social• Político• Legal, reglamentario• Financiero, económico• Tecnológico• Natural y competitivo
Interno Organización	<ul style="list-style-type: none">• Gobierno corporativo• Estructura de la organización y funciones• Políticas, objetivos y estrategias• Recursos y conocimientos• Sistemas de información• Cultura de la organización• Relaciones contractuales

4. Contexto de la organización

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización **debe** determinar:

- a) las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información;
- b) los requisitos relevantes de estas partes interesadas;
- c) cuales de estos requisitos se abordarán a través del sistema de gestión de la seguridad de la información.

Parte interesada: persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad.

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

(fuente: ISO/IEC 27000:2018)

Partes interesadas...



Necesidades y expectativas...

Contexto	Aspecto	Parte Interesada	Requisito
Interno	Relaciones contractuales	Proveedores CLOUD	Disponibilidad
Externo	Legal	Min. Secretaría General de la Presidencia	Ley 19628 Sobre protección de datos de carácter personal.



Organización

Partes Interesadas



4. Contexto de la organización

4.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La organización **debe** determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización **debe** considerar:

- a) las cuestiones externas e internas referidas en el apartado 4.1;
 - b) los requisitos referidos en el apartado 4.2;
 - c) las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras orga
- El alcance **debe** estar disponible como información documentada.

Documento
requerido

4. Contexto de la organización

4.3 Determinar el alcance del sistema de gestión de la seguridad de la información

¡Determinar qué se quiere proteger!



Documento
requerido

Alcance del SGSI: El alcance de un sistema de gestión puede incluir a toda la organización, una parte específica y/o funciones identificadas de la organización, o una o más funciones en un grupo de organizaciones.

Una organización externa está fuera del alcance del SGSI, aunque la función o proceso tercerizado esté dentro del alcance

(fuente: ISO/IEC 27000:2018)

LOS SISTEMAS DE INFORMACIÓN QUE DAN SOPORTE A LA INFORMACIÓN DE LAS ACTIVIDADES DE NEGOCIO DE: COMERCIALIZACIÓN, CONSULTORÍA, FORMACIÓN, PUESTA EN MARCHA Y MANTENIMIENTO DE SOLUCIONES SOFTWARE DE GESTIÓN EMPRESARIAL, DE ACUERDO A LA DECLARACIÓN DE APLICABILIDAD DE 09/10/2015.

“El sistema de gestión para la prestación de servicios (de TI) de *hosting, housing*, correo colaborativo y mantenimiento correctivo/preventivo de aplicaciones tipo ERP, de acuerdo al catálogo de servicios vigente.”

Sistema de Gestión de Seguridad de la Información aplicado a la información e infraestructuras que soportan los servicios de diseño, desarrollo y mantenimiento de aplicaciones y sistemas relacionados con la Verificación de Identidad.

Los Sistemas de información que dan soporte a la infraestructura tecnológica para la presentación de servicios de Mesa de Ayuda según la declaración de aplicabilidad en vigor a la fecha de emisión del certificado.

4. Contexto de la organización

4.4 Sistema de gestión de la seguridad de la información

La organización **debe** establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, incluyendo los procesos requeridos y sus interacciones de acuerdo con los requisitos de esta norma.

Garantizar que las organizaciones realizan una correcta gestión de la seguridad de la información mediante un proceso sistemático, documentado, conocido y adoptado por toda la organización, basado en un enfoque de gestión de riesgos.

4. Contexto de la organización

4.4 Sistema de gestión de la seguridad de la información

En esta cláusula se **incorpora el requisito de identificar los procesos necesarios y sus interacciones dentro del SGSI** que se requieren para su implementación y mantenimiento.

El SGSI debe basarse en procesos establecidos y trazables y en sus interacciones.

Los controles de seguridad de la información del Anexo A se diseñan y adaptan en torno a estos procesos.

Capítulos de Requisitos:

4. Contexto de la organización.

5. Liderazgo.

6. Planificación.

7. Apoyo.

8. Operación.

9. Evaluación de desempeño

10. Mejora

5. Liderazgo



5.1 Liderazgo y compromiso

La alta dirección **debe** demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información al:

- a) asegurando que **se establecen la política y los objetivos de seguridad de la información** y que estos sean compatibles con la dirección estratégica de la organización;
- b) asegurando la **integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización**;
- c) asegurando que los **recursos necesarios** para el sistema de gestión de la seguridad de la información **estén disponibles**;
- d) **comunicando** la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información;

5. Liderazgo



5.1 Liderazgo y compromiso

(continuación)

- e) asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos;
- f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;
- g) promoviendo la mejora continua; y
- h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

Obligaciones que debiera demostrar la dirección de la organización.

5.1 Liderazgo y compromiso

Cómo llevarlo a la práctica...

La alta dirección de una organización debiera:

- Definir las expectativas sobre lo que se espera del sistema de seguridad de la información.
- Establecer cuál será la postura de riesgo de la organización frente a que riesgos se aceptarán y cuales no.
- Compromiso: “A mayor jerarquía mayor exigencia”.
- Asegurar los recursos necesarios para implementar una estrategia de seguridad que logre alcanzar las expectativas establecidas.
- ...

Las soluciones tecnológicas no lo son todo en seguridad.

Un liderazgo bien planteado debiera definir y verificar las responsabilidades para cada trabajador de forma que se pueda realizar un trabajo seguro.

5. Liderazgo

5.2 Política

La alta dirección **debe** establecer una política de seguridad de la información que:

- a) sea **adecuada** al propósito de la organización;
- b) incluya** objetivos de seguridad de la información (véase 6.2) **o proporcione un marco de referencia** para el establecimiento de los objetivos de seguridad de la información;
- c) incluya el **compromiso de cumplir con los requisitos aplicables** a la seguridad de la información; e
- d) incluya el **compromiso de mejora continua** del sistema de gestión de la seguridad de la información.

5. Liderazgo

5.2 Política

(continuación)

La política de seguridad de la información **debe**:

- e) estar disponible como información documentada;
- f) ser **comunicada** dentro de la organización; y
- g) **estar disponible** para las partes interesadas, según sea apropiado.



Documento
requerido

5. Liderazgo

Una política de seguridad de la información coherente y adecuada debería:

- Proporcionar una directriz clara sobre el tratamiento de la seguridad de la información en la organización.
- Indicar los objetivos de este sistema.
- Incluir un compromiso de cumplir con los requisitos u objetivos comerciales y con los requisitos contractuales, legales o reglamentarios.
- Asumir un compromiso de mejorar continuamente el SGSI.
- Asignar responsables de las operaciones, de la coordinación en el día a día, de la ejecución general, de la evaluación de riesgos y de la práctica de auditorías, inspecciones e investigación de incidentes.

Pero en el marco de la seguridad de la información

5. Liderazgo

Política (ej.)



La Dirección General de la UNIDAD ADMINISTRATIVA ESPECIAL MIGRACIÓN COLOMBIA, como autoridad migratoria del estado colombiano, se compromete a proteger los principales activos de información para preservar su confidencialidad, integridad y disponibilidad, a través del mejoramiento continuo de la gestión institucional y el cumplimiento de los requisitos aplicables, mediante la gestión de los riesgos de la seguridad de la información, incluyendo la ciberseguridad y la protección de los datos personales, y la toma de conciencia de nuestras partes interesadas.

5. Liderazgo

5.3 Roles, responsabilidades y autoridades en la organización

La alta dirección **debe** asegurarse que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección **debe** asignar la responsabilidad y autoridad para:

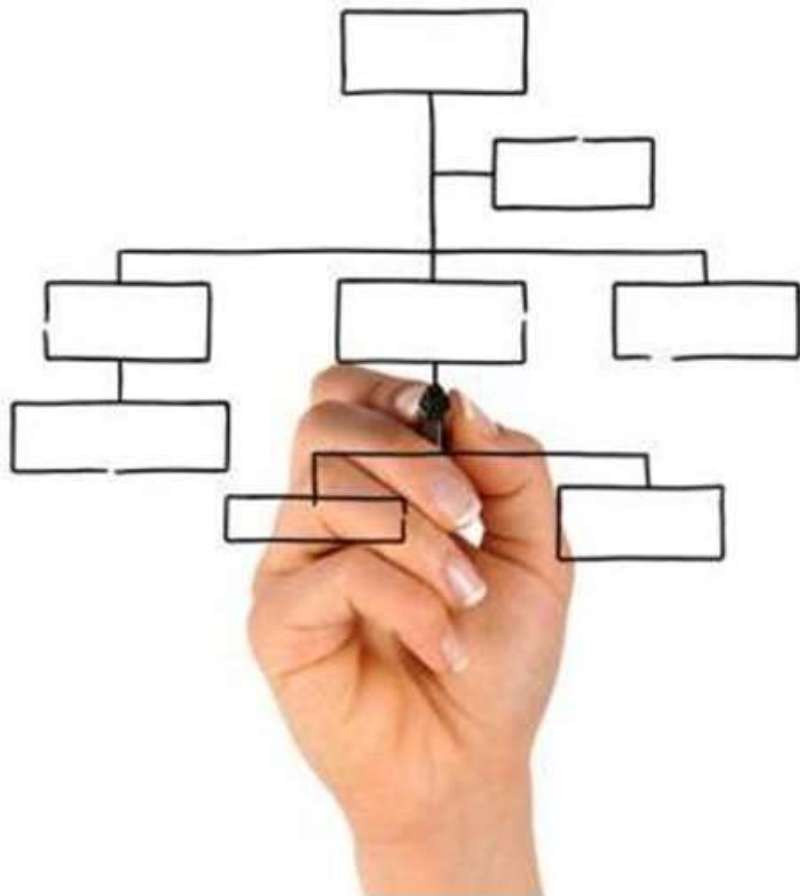
- a) asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de este documento;
- b) informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información.

5. Liderazgo

Roles, responsabilidades y autoridades en la organización

- Definir actividades asignadas a responsables (**quién hace qué**).
- Determinar autoridades en caso de requerir la toma de alguna decisión respecto de la seguridad de la información (**quién autoriza, concede, prohíbe, decide, etc., sobre algún activo de información**).
- Establecer la figura de un Coordinador de Seguridad de la Información (CISO = Chief Information Security Officer) o asignar esta autoridad y responsabilidad en alguno de los cargos de la organización.

ISO 27001 no requiere un CISO, pero es recomendable tenerlo.



Establecer un organigrama con las funciones de seguridad de la información o incluir dichas funciones en los cargos del organigrama ya existente.

Descriptor de Cargo: Componentes, deberes, requisitos y responsabilidades exigidas por el puesto a través de la aplicación de uno o más métodos

Perfil de Cargo: Método de recopilación de los requisitos de cualificaciones personales, es decir las competencias exigidas para el cumplimiento satisfactorio de las tareas de un colaborador dentro de la organización.

Capítulos de Requisitos:

4. Contexto de la organización.

5. Liderazgo.

6. Planificación.

7. Apoyo.

8. Operación.

9. Evaluación de desempeño

10. Mejora

6 Planificación

6.1 Acciones para abordar los riesgos y las oportunidades

6.1.1 Consideraciones generales - Al planificar el SGSI, la organización **debe** considerar las cuestiones a las que se hace referencia en el apartado 4.1 y los requisitos incluidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:

- a) asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos;
- b) prevenir o reducir efectos indeseados;
- c) lograr la mejora continua.

6 Planificación

6.1.1 Consideraciones generales (cont)

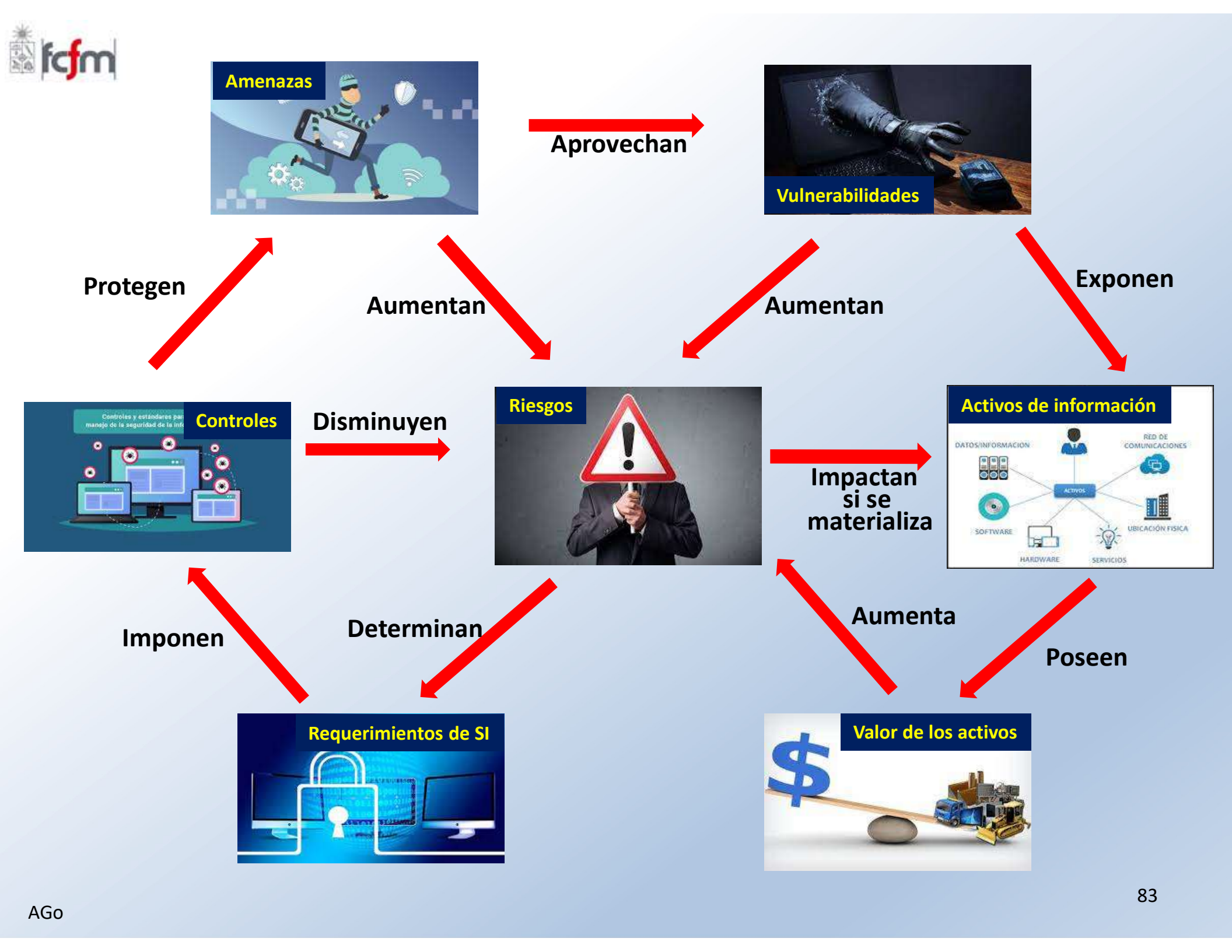
La organización **debe** planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

- 1) **integrar e implementar** las acciones en los procesos del sistema de gestión de la seguridad de la información, y
- 2) **evaluar la eficacia** de estas acciones.

**Pero sobre qué elementos se debe
abordar los riesgos y oportunidades...**



Gestión del riesgo



**No olvidar abordar también
las oportunidades**

Por lo general, las oportunidades identificadas en el Análisis de Contexto y en la Partes Interesadas, son abordadas en la Revisión por la Dirección.

6 Planificación

6.1.2 Evaluación de los riesgos de seguridad de la información

La organización **debe definir y aplicar un proceso de evaluación de los riesgos** de seguridad de la información que:

- a) establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
 - 1) los criterios de aceptación de los riesgos, y
 - 2) los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información;
- b) asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables;

6 Planificación

6.1.2 Evaluación de los riesgos de seguridad de la información (continuación)

- c) identifique los riesgos de seguridad de la información:
 - 1) llevando a cabo el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información,
 - 2) identificando a los dueños de los riesgos;
- d) analice los riesgos de seguridad de la información:
 - 1) valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto 6.1.2 c) 1) llegasen a materializarse,
 - 2) valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto 6.1.2 c) 1),
 - 3) determinando los niveles de riesgo;

6 Planificación

6.1.2 Evaluación de los riesgos de seguridad de la información (continuación)

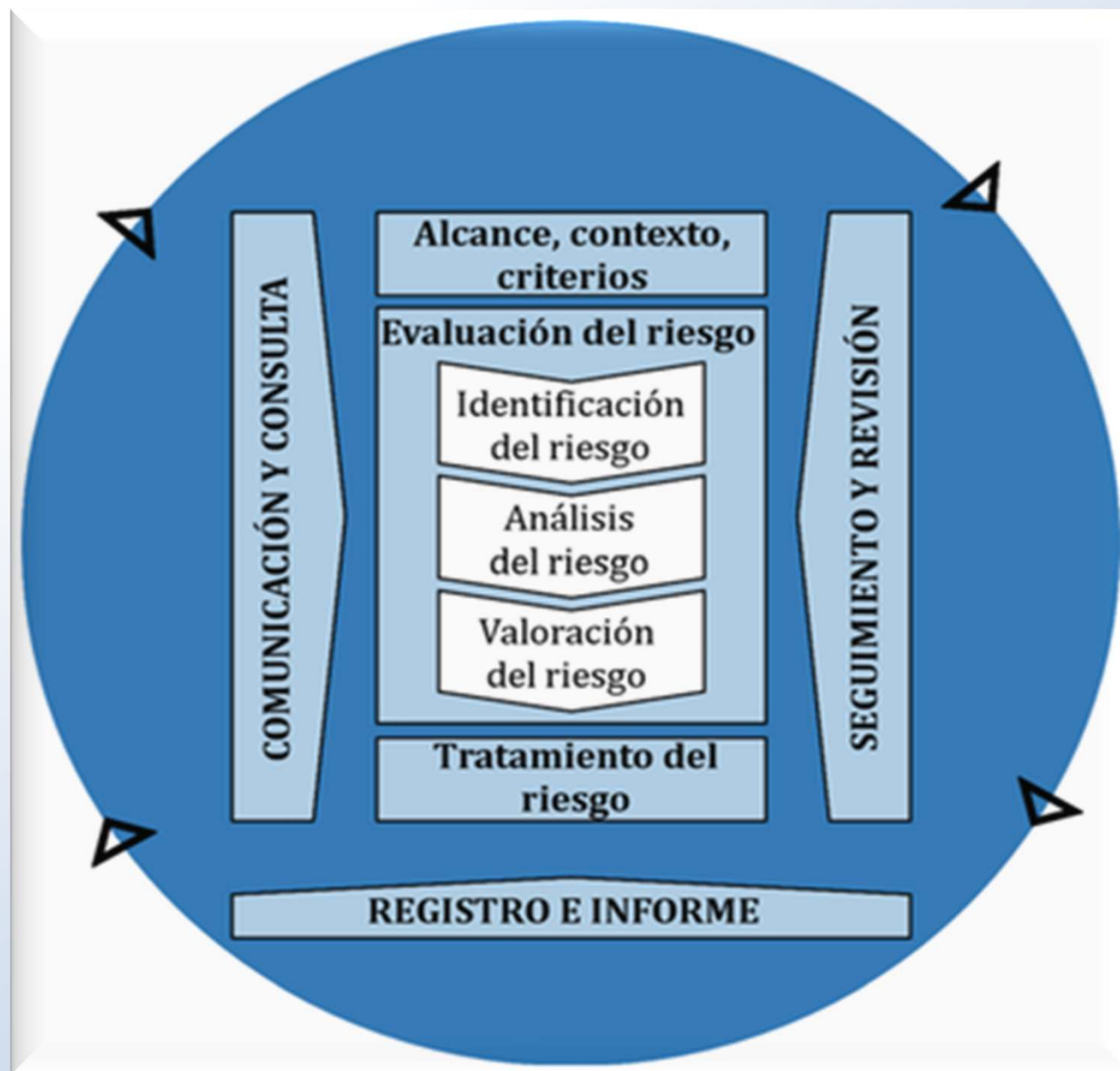
- e) evalúe los riesgos de seguridad de la información:
- 1) comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos en el punto 6.1.2 a),
 - 2) priorizando el tratamiento de los riesgos analizados.

La organización **debe conservar información documentada** sobre el proceso de apreciación de riesgos de seguridad de la información.



Evidencia
requerida

Gestión del riesgo



6 Planificación

6.1.3 Tratamiento de los riesgos de seguridad de la información

La organización **debe** definir y efectuar un proceso de tratamiento de los riesgos de seguridad de la información para:

- a) seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos;
- b) determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;
- c) comparar los controles determinados en el punto 6.1.3 b) con los del anexo A y comprobar que no se han omitido controles necesarios;

6 Planificación

6.1.3 Tratamiento de los riesgos de seguridad de la información (continuación)

- d) elaborar una “Declaración de Aplicabilidad” que contenga:
 - los controles necesarios [véase 6.1.3 b) y c)];
 - la justificación de las inclusiones;
 - si los controles necesarios están implementados o no; y
 - la justificación de las exclusiones de cualquiera de los controles del anexo A;
- d) formular un plan de tratamiento de riesgos de seguridad de la información; y
- e) obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.



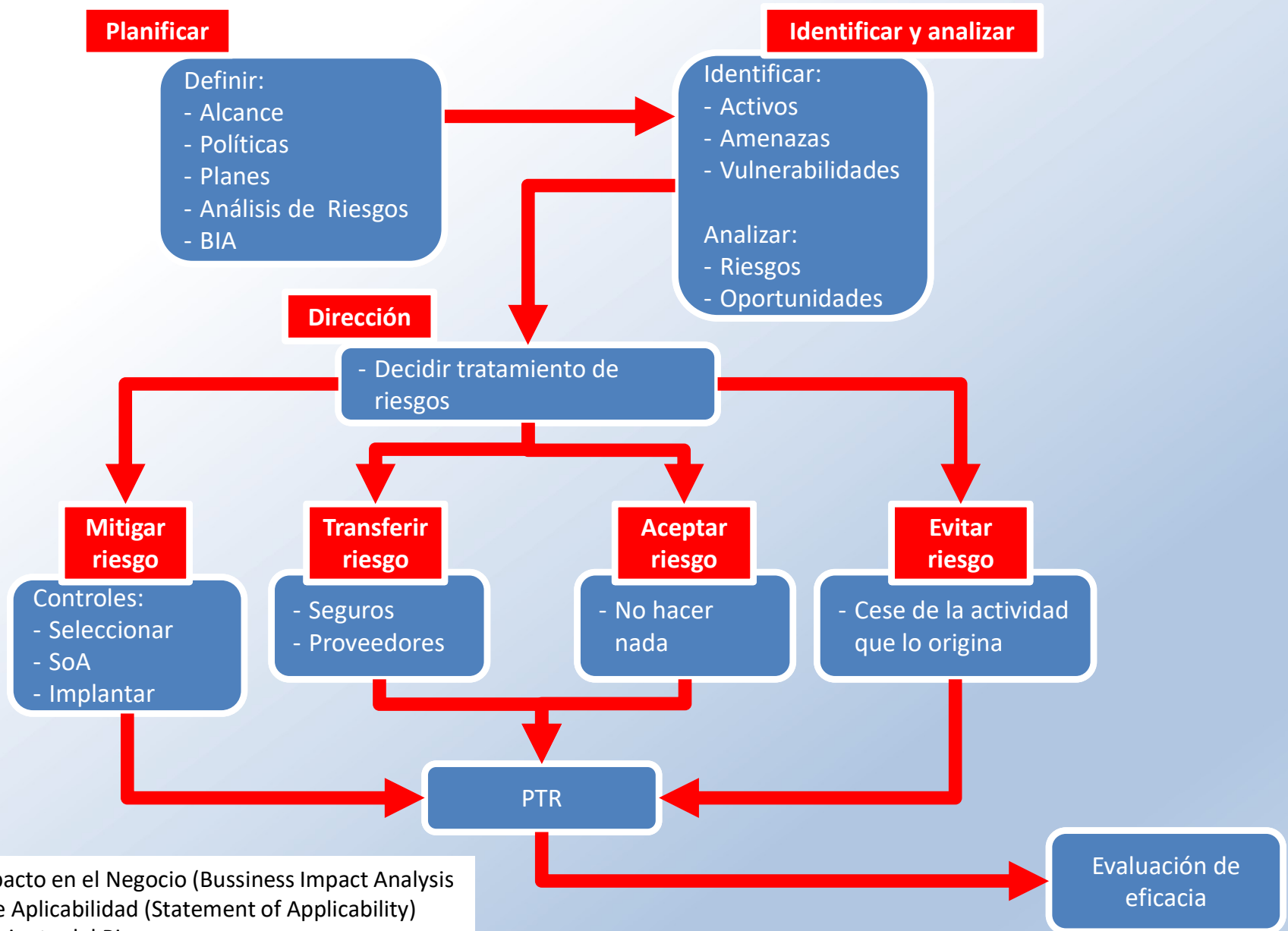
**Documento
requerido**

La organización **debe** conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.



**Evidencia
requerida**

Gestión del riesgo



BIA = Análisis de Impacto en el Negocio (Business Impact Analysis)
 SoA = Declaración de Aplicabilidad (Statement of Applicability)
 PTR = Plan de Tratamiento del Riesgo

La seguridad total



¡No existe!

Evaluación de riesgos de la SI

¿Por qué no se gestionan los Riesgos en las Organizaciones?

- No aporta valor...
- Si pensamos en todo lo malo, no hacemos nada.
- Hay suficientes controles.
- Aquí pensamos en metas, no en riesgos.
- Aceptamos que es común que fallen los sistemas tecnológicos.
- No hay tiempo para evaluar los riesgos, necesitamos vender
- Acá nunca pasó nada.
- No tenemos los procesos definidos.
- Gestionar los riesgos no me va a ayudar a vender más.
- Si ocurre algo, ya lo arreglaremos.

Evaluación de riesgos de la SI

Diferentes tipos de Gestión de Riesgos en las Organizaciones

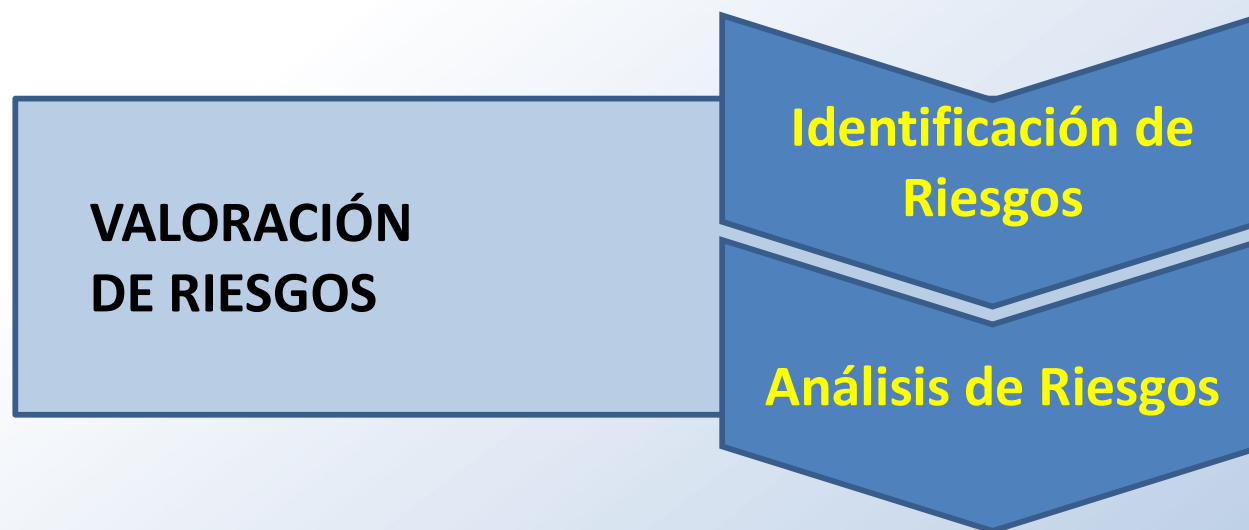


Evaluación de riesgos de la SI

El proceso de gestión de riesgos involucra cuatro actividades cíclicas:

1. la identificación de activos y los riesgos a los que están expuestos
2. el análisis de los riesgos identificados para cada activo
3. la selección e implantación de controles que reduzcan los riesgos
4. el seguimiento, medición y mejora de las medidas implementadas

Evaluación de riesgos de la SI



Riesgos de seguridad de la información pueden ser expresados como efecto de la incertidumbre sobre los objetivos de la seguridad de la información.

Notas:

- Efecto es una desviación de lo esperado: positivo o negativo.
- Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de un evento, su consecuencia o probabilidad.
- El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causar daño a una organización.

Evaluación de riesgos de la SI

Cómo clasificar activos de información

- Criticidad de un activo en función de cuán necesario resulta para las actividades de un área o la misión de la organización.
- No todos los activos de información poseen el mismo valor,
- Un mismo activo puede poseer un valor diferente para distintas áreas,
- Establecer una valoración estandarizada donde el propietario de la información clasifica cada activo según las tres características básicas de la seguridad de la información: **confidencialidad, integridad, y disponibilidad** a la que debe estar sometido.

Clasificación de activos

CONFIDENCIALIDAD	VALOR
Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la organización.	0
Información que puede ser conocida y utilizada por todos los agentes de la organización	1
Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.	2
Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la organización o a terceros.	3

INTEGRIDAD	VALOR
Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la organización.	0
Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para la organización o terceros.	1
Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la organización o terceros.	2
Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades	3

DISPONIBILIDAD	VALOR
Información cuya inaccesibilidad no afecta la actividad normal de la organización.	0
Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la organización.	1
Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la organización.	2
Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la organización.	3

Clasificación de activos

El valor máximo de las tres características determinará la criticidad del activo de información analizado.

- Si todos son 0 = Criticidad 0 = Nula
- Si el máximo es 1 = Criticidad 1 = Baja
- Si el máximo es 2 = Criticidad 2 = Media
- Si el máximo es 3 = Criticidad 3 = Alta

Ejemplo:

Activo	Confiden.	Integridad	Dispo.	Criticidad
Bases de Datos	3	2	1	3
Red de telecomunicaciones	0	1	1	1

Declaración de Aplicabilidad

Tabla A.1 – Controles de la seguridad de la información

5	Controles organizacionales	
5.1	Políticas para la seguridad de la información	<p>Control</p> <p>La política de seguridad de la información y un conjunto de políticas temáticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.</p>
5.2	Roles y responsabilidades en seguridad de la información	<p>Control</p> <p>Todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.</p>
5.3	Segregación de tareas	<p>Control</p> <p>Las funciones y áreas de responsabilidad en conflicto deben segregarse.</p>

Para cada control se deberá declarar:

- su aplicabilidad al SGSI y justificación de por qué aplica o no.
- Método establecido por la organización para dar cuenta del control

Recomendación de controles

El resultante de lo planteado en 6.1.2 (Evaluación de los riesgos de SI) constituye un **detalle de los riesgos a los que el sistema está expuesto**, otorga un **orden de prioridad de los riesgos a tratar**.

Los activos con alto nivel de riesgo son los que **debieran ser tratados en el corto plazo**; los riesgos de nivel medio también son relevantes, pero suelen tratarse a más largo plazo; finalmente los riesgos de bajo nivel suelen aceptarse.

La recomendación de controles **incluye la identificación de medidas adecuadas que mitiguen o eliminen los riesgos** detectados previamente.

Un control contribuye **reduciendo el impacto** que produce una amenaza o bien **la frecuencia** con la que ésta sucede.

El objetivo es **reducir el nivel de riesgo** al que el sistema está expuesto, llevándolo a un **nivel aceptable**.

Recomendación de controles

Activo	Confiden.	Integridad	Dispo.	Criticidad
Bases de Datos	3	2	1	3
Red de telecomunicaciones	0	1	1	1

Activo	Criticidad	Amenaza/Riesgo	Control
Bases de Datos	3	Pérdida de datos	<ul style="list-style-type: none"> - Copias de seguridad - Capacitación al usuario - Restricción de permisos
		Falla en discos duros del servidor	<ul style="list-style-type: none"> - Copias de seguridad - Mantenimiento preventivo - Migración de BdD a CLOUD

Incluir la identificación del propietario del activo en riesgo y la aprobación del plan de tratamiento del riesgo

**Evidencia
requerida**

6 Planificación

6.2 Objetivos de seguridad de la información y planificación para lograrlos

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

Los objetivos de seguridad de la información **deben**:

- a) ser coherentes con la política de seguridad de la información;
- b) ser medibles (si es posible);
- c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos;
- d) ser monitorizados;
- e) ser comunicados;
- f) ser actualizados, según sea apropiado;
- g) estar disponibles como información documentada.

6 Planificación

6.2 Objetivos de seguridad de la información y planificación para lograrlos

(continuación)

La organización **debe** **conservar inform**  **entada** sobre los objetivos de seguridad de la información.

Cuando se hace la planificación para la consecución de los objetivos de seguridad de la información, la organización **debe** determinar:

- h) lo que se va a hacer;
- i) qué recursos se requerirán;
- j) quién será responsable;
- k) cuando se finalizará; y
- l) cómo se evaluarán los resultados.

Objetivos de SI y su planificación

Ejemplo de objetivo y su planificación:

- Tratar los riesgos operacionales y estratégicos en seguridad de la información para que permanezcan en niveles aceptables para la organización (**no tener riesgos críticos identificados sin tratamiento eficaz, evaluación anual**).

Responsabilidades:

- Cada gerente es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

Indicadores:

- Los incidentes en seguridad de la información no se traducirán en costos graves e inesperados, o en una grave perturbación de los servicios y actividades comerciales.

Objetivos de SI y su planificación

Ejemplo de objetivo y su planificación:

- Confidencialidad de datos: Disponibilidad de información solo para usuarios, procesos y dispositivos autorizados.
- Acciones:
 - Restricción o cierre completo del acceso a la información
 - Cifrado
 - Evitar almacenamiento disperso
 - No publicar la existencia de información

Responsabilidades:

- Cada gerente es responsable de garantizar que las personas que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la organización.

Indicadores:

- Cantidad de vulneraciones a la confidencialidad de la información en un período dado.

6 Planificación

6.3 Planificación de cambios

Cuando la organización determine la necesidad de cambios en el sistema de gestión de la seguridad de la información, estos cambios se **deben** llevar a cabo **de manera planificada**.



Antes de implementar algún cambio:

- Entender por qué el cambio es necesario.
- Cuál es el impacto en el riesgo al que se está expuesto el SGSI debido al cambio.
- ¿Están los nuevos recursos disponibles?
- ¿Será necesario asignar o reasignar las nuevas responsabilidades?
- Otras consideraciones.

Capítulos de Requisitos:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
- 7. Apoyo.**
8. Operación.
9. Evaluación de desempeño
10. Mejora

7 Apoyo

7.1 Recursos

La organización **debe** determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.



Cuando se habla de recursos será necesario incluir a las personas, los ambientes para la operación de proceso, la infraestructura, los recursos de seguimiento, conocer la organización, etc.

7.1 Recursos

Determinar y proporcionar significa identificar qué es necesario y como serán suministrados esos recursos (compra, arriendo, tercerización, etc.).

Queda claro que la seguridad de la información no es gratis. Será necesario un cierto nivel de inversión acorde con la evaluación de riesgos y sobre todo con los criterios para asumir o minimizar los distintos niveles de riesgo del SGSI teniendo en cuenta:

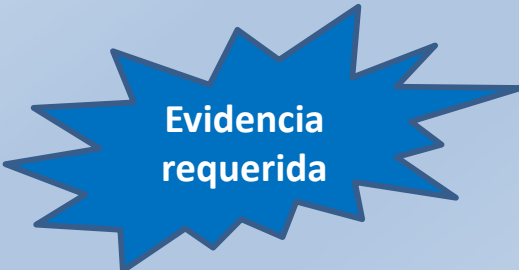
- La inversión económica.
- Las dependencias actuales
- Los equipos que contengan información
- Las personas de la organización o terceros implicados
- Etc.

7 Apoyo

7.2 Competencias

La organización **debe**:

- a) determinar las competencias necesarias de las personas que trabajan bajo su control que afecta a su desempeño en seguridad de la información; y
- b) asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;
- c) cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo; y
- d) **conservar la información documentada apropiada,** como evidencia de la competencia..



Evidencia
requerida

7.2 Competencia

Al contratar una persona para un rol de SI específico, las organizaciones deberían asegurarse de que el candidato:

- a) cuente con las competencias necesarias para desempeñar el rol de seguridad;
- b) sea confiable para asumir el rol, en especial si éste es fundamental para la organización.

Descriptor de Cargo: Componentes, deberes, requisitos y responsabilidades exigidas por el puesto a través de la aplicación de uno o más métodos

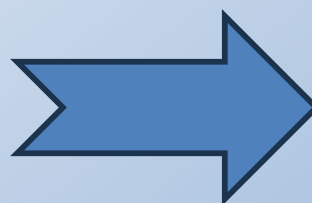
Perfil de Cargo: Método de recopilación de los requisitos de cualificaciones personales, es decir las competencias exigidas para el cumplimiento satisfactorio de las tareas de un colaborador dentro de la organización.

7 Apoyo

7.3 Concienciación (toma de conciencia)

Las personas que trabajan bajo el control de la organización **deben** ser conscientes de:

- a) la política de la seguridad de la información;
- b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; y
- c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.



7.3 Concienciación (toma de conciencia)

Los puntos concretos a tener en cuenta podrían ser:

1. Establecer un programa de formación y sensibilización o concienciación.
2. Programar distintas actividades de sensibilización.
3. Utilizar todos los medios de comunicación a su alcance.
4. Mantener informados a todos de las actualizaciones en temas de seguridad tomando en cuenta lo aprendido en los incidentes de seguridad de la información,
5. Realizar simulaciones de incidentes de seguridad (correo phishing, etc.).

7 Apoyo

7.4 Comunicación

La organización **debe** determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

- a) el contenido de la comunicación;
- b) cuándo comunicar;
- c) con quién comunicar;
- d) cómo comunicar..



- Comunicación a las partes interesada de la visión de seguridad de la información incluido:
 - Por qué es necesario el SGSI.
 - Cuáles son las responsabilidades legales de la organización.
 - Cómo afecta a cada empleado y sección de la empresa cuando el programa esté implantado.



7 Apoyo

7.5 Información documentada

7.5.1 Consideraciones generales

El sistema de gestión de la seguridad de la información de la organización **debe** incluir:

- a) la información documentada requerida por este documento;
- b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

7 Apoyo

7.5.2 Creación y actualización

Cuando se crea y actualiza la información documentada, la organización **debe** asegurarse, en la manera que corresponda, de lo siguiente:

- a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
- b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);
- c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7 Apoyo

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por este documento se **debe** controlar para asegurarse que:

- a) esté disponible y preparada para su uso, dónde y cuándo se necesite;
- b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

7 Apoyo

7.5.3 Control de la información documentada (continuación)

Para el control de la información documentada, la organización **debe** tratar las siguientes actividades, según sea aplicable:

- c) distribución, acceso, recuperación y uso;
- d) almacenamiento y preservación, incluida la preservación de la legibilidad;
- e) control de cambios (por ejemplo, control de versión);
- f) conservación y disposición.

La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de la calidad, se **debe** identificar, según sea apropiado, y controlar.

7.5 Información documentada

Información documentada mantenida y conservada en lugar de “documentos y registros”.

Este requisito se relaciona con la creación y actualización de información documentada y con su control. Ya no se requiere un procedimiento documentado ni una lista de documentos, la revisión ISO 27001:2022 pone el énfasis en el contenido en lugar del título de la forma del documento. Ahora bien, podemos llevarnos a engaño si pensamos que no se requiere documentación en la nueva norma. Tener en cuenta que los requisitos para la información documentada se presentan en cada la cláusula a la que hacen referencia.



Documentación requerida

Cláusula	Información
4.3	Alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Proceso de evaluación de riesgos de seguridad de la información
6.1.3	Proceso de tratamiento de riesgos de seguridad de la información
6. 1.3 d)	Declaración de aplicabilidad
6.2	Objetivos de seguridad de la información
7.2 d)	Evidencias de competencia
7.5.1 b)	Información documentada determinada como necesaria para la efectividad del SGSI
8.1	Control y planificación operacional
8.2	Resultados de la evaluación de riesgos de seguridad de la información
8.3	Resultados del tratamiento de riesgo de seguridad de la información
9.1	Evidencia de los resultados del seguimiento y medición
9.2	Evidencia de la implementación del programa de auditoría y de los resultados de auditorías
9.3.3	resultados de las revisiones por la dirección
10.1 f) y g)	Evidencia de la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y los resultados de cualquier acción correctiva.

Documentación requerida

Control	Información
A.5.1	Políticas temáticas específicas para la seguridad de la Información
A.5.7	Información relativa a las amenazas a la seguridad de la información.
A.5.9	Inventario de información y otros activos asociados.
A.5.10	Reglas para el uso aceptable y procedimientos para el manejo de información.
A.5.13	Procedimientos para etiquetar la información según esquema de clasificación
A.5.14	procedimientos o acuerdos de transferencia de información
A.5.20	Requisitos de seguridad de la información con cada proveedor.
A.5.24	Procedimientos documentados para la gestión de incidentes de SI.
A.5.28	Procedimiento para identificar, recoger, adquirir y preservar evidencias relacionadas con eventos de SI.
A.5.31	Identificación de requisitos legales, reglamentarios y Contractuales
A.5.34	identificar los requisitos relativos a la preservación de la privacidad y la protección de datos de carácter personal
A.5.37	procedimientos operacionales de los medios de tratamiento de la información
A.6.2	Términos y condiciones de Contratación

Documentación requerida

Control	Información
A.6.6	Acuerdos de confidencialidad o no divulgación con el personal y otras partes interesadas
A.8.8	información acerca de las vulnerabilidades técnicas de los sistemas de información utilizados.
A.8.9	Gestión de la configuración.
A.8.19	Procedimiento para Instalación del software en sistemas en producción
A.8.27	principios de ingeniería de sistemas seguros

Capítulos de Requisitos:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Apoyo.
- 8. Operación.**
9. Evaluación de desempeño
10. Mejora

8. Operación

8.1 Planificación y control operacional

La organización **debe** planificar, implementar y controlar los **procesos necesarios** para cumplir los requisitos, y para implementar las acciones determinadas en el capítulo 6:

- **estableciendo criterios para los procesos;**
- implementando controles en los procesos de acuerdo con los criterios.

En la medida necesaria la organización **debe** tener disponible **información documentada**, para tener la confianza de que los procesos se han llevado a cabo según lo planificado.

La organización **debe** controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario.

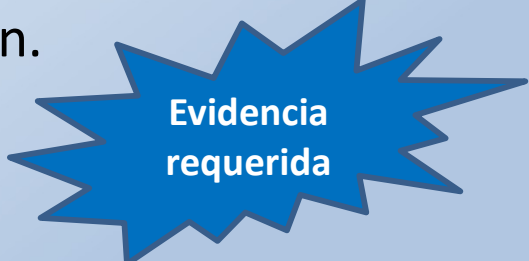
La organización **debe** garantizar que los procesos, productos o servicios proporcionados externamente y relevantes para el sistema de gestión de la seguridad de la información estén controlados.

8. Operación

8.2 Evaluación de los riesgos de seguridad de la información

La organización **debe** efectuar evaluaciones de riesgos de seguridad de la información a intervalos planificados, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a).

La organización **debe** conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.



Evidencia
requerida

Criterios en 6.1.2.a)

- los criterios de aceptación del riesgo;
- los criterios para realizar las evaluaciones de riesgo de la seguridad de la información.

8.2 Evaluación de los riesgos de seguridad de la información

El riesgo de la SI más grande es creer que la información está segura, sin verificarlo. Es frecuente que la empresa que han sufrido algún tipo de daño en su información sea por dos causas principales:

- Creer que se está seguro.
- Relajamiento en el comportamiento del personal.

La evaluación de riesgos de SI consta de **identificar, analizar y evaluar** los riesgos existentes en una organización dentro de su contexto particular.

Ayuda a garantizar que los controles de seguridad que elija una organización para anular o mitigar el riesgo encontrado **sean adecuados** y a realizar un **seguimiento permanente** de ellos mediante la implementación de políticas, procedimientos y/o de medios tecnológicos, con el objetivo de **disminuir significativamente la posibilidad** de que el riesgo sea una realidad.

8.2 Evaluación de los riesgos de seguridad de la información

Es la puesta en práctica de lo determinado en 6.1.2.
Pero cómo evaluar...

Mediante:

- Auditorías al cumplimiento de las políticas de seguridad de la información y a las políticas temáticas especializadas además de la verificación de la eficacia de los controles establecidos.
- Herramientas informáticas tales como:
 - Software antimalware.
 - Firewalls
 - Control de acceso
 - Software y hardware actualizado
 - Monitoreo de redes
 - Uso de VPNs
 - Escáner de vulnerabilidades.
 - Cifrado de datos en los equipos.
 - Pruebas de penetración.
 - Etc.



8. Operación

8.3 Tratamiento de los riesgos de seguridad de la información

La organización **debe** implementar el plan de tratamiento de los riesgos de seguridad de la información.

La organización **debe** conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.

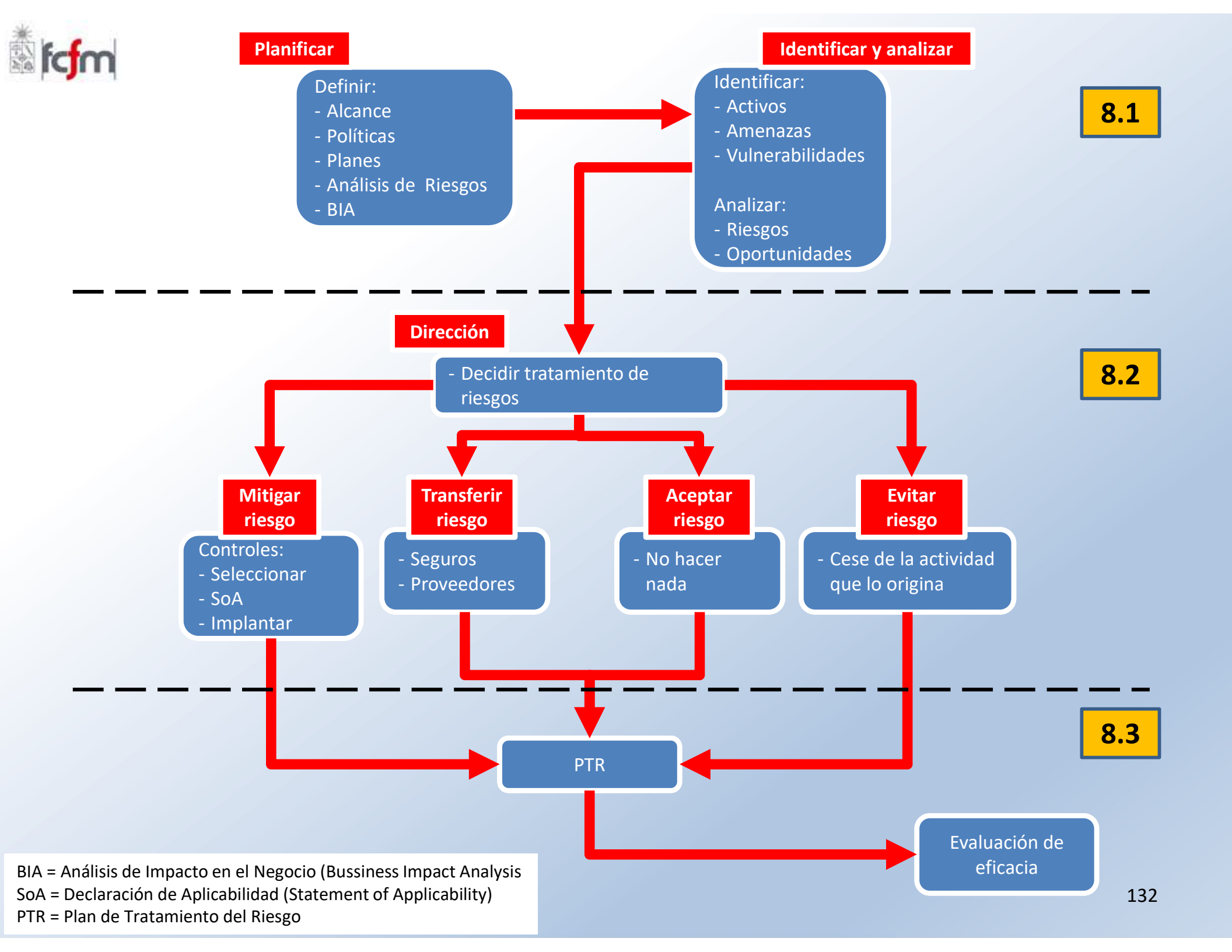


Evidencia
requerida

Ver lo establecido en 6.1.3

8.3 Tratamiento de los riesgos de seguridad de la información

Nombre del Riesgo	Causas	Consecuencias	Control	Acción de contingencia ante posible materialización
Pérdida de Confidencialidad	Cultura de inseguridad (desconocimiento de buenas prácticas)	Procesos disciplinarios	El jefe de la Oficina Asesora de Planeación cada dos meses vela por el cumplimiento y la efectividad de la campaña de sensibilización en seguridad de la información. En caso de desviación se revalúa la estrategia de la campaña. Se evidencia su implementación mediante piezas, actas de reunión y reportes.	1. Activar el procedimiento de gestión de incidentes.
	Colaboradores que divulgan la información	Deterioro del clima laboral de la Entidad	La Coordinadora del Grupo de Mejoramiento durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a través de la documentación de las políticas de operación y del SIG. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución a través de la documentación en Intranet.	2. Reportar a las instancias pertinentes el caso.
	Claves genéricas	Imposibilidad de determinar responsable de la divulgación	La Coordinadora del Grupo de Mejoramiento durante la vigencia, oficializa los lineamientos de protección de propiedad intelectual y preservación de la confidencialidad de la información de la Entidad, a través de la documentación de las políticas de operación y del SIG. En el caso que los lineamientos de operación no sean adoptados por los usuarios, se revisará la estrategia de socialización. Se evidencia su ejecución a través de la documentación en Intranet.	3. Solicitar el cambio inmediato de la contraseña o en caso extremo la inhabilitación de la contraseña.
	Divulgaciones no autorizadas de claves	Imposibilidad de determinar responsable de la divulgación	El Oficial de Seguridad de la Información durante la vigencia, implementará la estrategia de sensibilización y documentación para el uso de contraseñas seguras. En caso	4. Activar el procedimiento de gestión de incidentes y



8.1

8.2

8.3

Capítulos de Requisitos:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Apoyo.
8. Operación.
- 9. Evaluación de desempeño**
10. Mejora

9. Evaluación de desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización **debe** determinar:

- a) a qué es necesario monitorizar y medir, incluyendo procesos y controles de seguridad de la información;
- b) los métodos de monitorización, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos;
- c) cuándo se deben llevar a cabo el seguimiento y la medición;
- d) quién debe hacer el seguimiento y la medición;
- e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;
- f) quién debe analizar y evaluar esos resultados.

9. Evaluación de desempeño

9.1 Seguimiento, medición, análisis y evaluación

(continuación)

La organización **debe** tener disponible la información documentada apropiada como evidencia de los resultados.

Evidencia
requerida

La organización **debe** **evaluar el desempeño** de la seguridad de la información y la **eficacia** del sistema de gestión de la seguridad de la información.



9.1 Seguimiento, medición, análisis y evaluación

Un desafío común para muchas organizaciones se encuentra en **decidir qué procesos deben incorporar indicadores de medición** para garantizar que las desviaciones en relación con los procesos del SGSI se detecten y aborden como parte de la mejora continua, así como elegir cómo medir y determinar cómo materializarlos.

Algunos indicadores pueden evaluar:

- Gestión del riesgo
- Control de la seguridad
- Ciclo de vida de los sistemas
- Planes de seguridad
- Seguridad en Recursos Humanos
- Protección física de las oficinas de trabajo
- Seguridad en el puesto de trabajo
- Control de la información saliente/entrante
- Continuidad del negocio
- Mantenimiento y actualización del hardware y software
- Documentación de las políticas, procesos, guías e instrucciones técnicas
- Concienciación de los empleados
- Respuesta ante incidentes

9.1 Seguimiento, medición, análisis y evaluación

La norma establece varios requisitos donde se debe evaluar resultados.

Medir la efectividad de los procesos de un SGSI es medir su desempeño contra un conjunto de objetivos u objetivos predefinidos, tales como desviaciones de los objetivos en números o porcentajes o hitos.



Al menos se debe evaluar lo establecido en
6.1.1.e).2; 6.2.l, 7.2.c, 10.2.b, A.5.22,
A.5.25, A.8.8, A.8.16

9. Evaluación de desempeño

9.2 Auditoría interna

9.2.1 Consideraciones generales

La organización **debe** llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) cumple con:

1. los requisitos propios de la organización para su sistema de gestión de la seguridad de la información,
2. los requisitos de este documento,

b) está implementado y mantenido de manera eficaz.

9. Evaluación de desempeño

9.2.2 Programa de auditoría interna

La organización **debe** planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes.

Al establecer el programa o programas de auditoría interna, la organización **debe** tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas.

9. Evaluación de desempeño

9.2.2 Programa de auditoría interna (continuación)

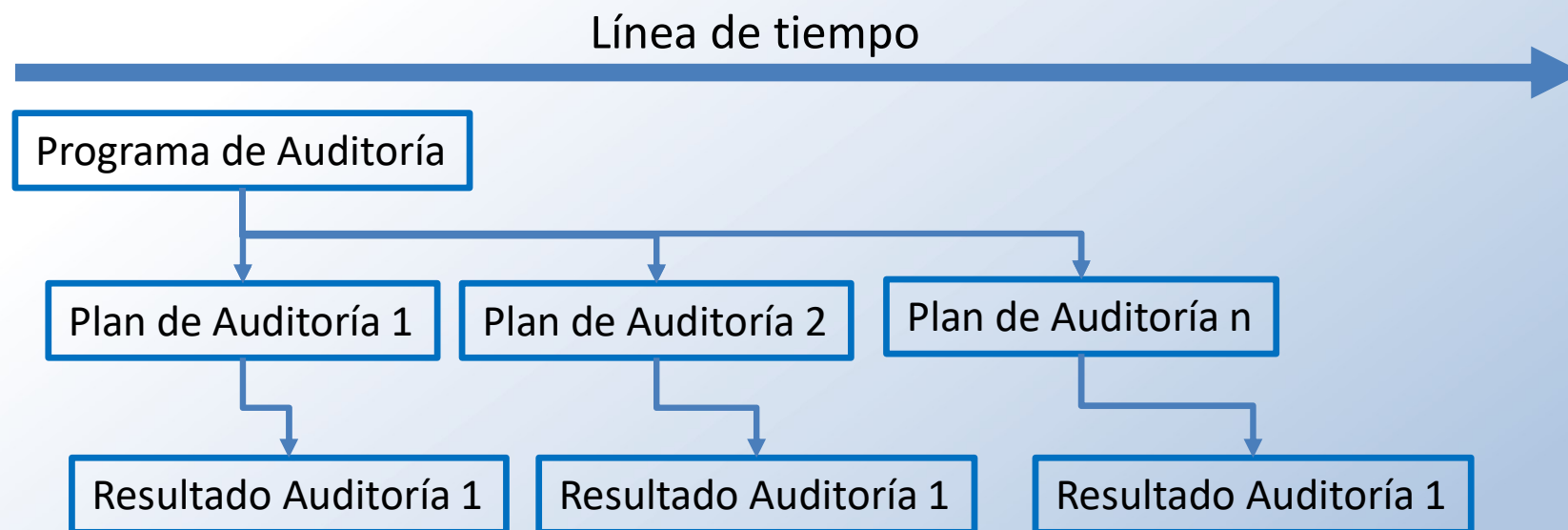
La organización **debe**:

- a) para cada auditoría, definir sus criterios y su alcance;
- b) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría; y
- c) asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías.

Se **debe** tener disponible información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.

Evidencia
requerida

9.2 Auditoría interna



9. Evaluación de desempeño

9.3 Revisión por la dirección

9.3.1 Consideraciones generales

La alta dirección **debe** revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección **debe** incluir consideraciones sobre:

- a) el estado de las acciones de anteriores revisiones por la dirección;
- b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;
- c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de la seguridad de la información;

9. Evaluación de desempeño

9.3.2 Entradas de la revisión por la dirección (continuación)

- d) la información sobre el comportamiento de la seguridad de la información, incluidas las tendencias relativas a:
 - 1) no conformidades y acciones correctivas,
 - 2) seguimiento y resultados de las mediciones,
 - 3) resultados de auditoría,
 - 4) el cumplimiento de los objetivos de seguridad de la información;
- e) los comentarios provenientes de las partes interesadas;
- f) los resultados de la evaluación de los riesgos y el estado del plan de tratamiento de riesgos;
- g) las oportunidades de mejora continua.

9. Evaluación de desempeño

9.3.3 Resultados de la revisión por la Dirección

Los resultados de la revisión por la dirección **deben** incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización **debe** tener disponible **información documentada** como evidencia de los resultados de las revisiones por la dirección.



Evidencia
requerida

ENTRADAS

- estado de las acciones de revisiones anteriores;
- cambios en cuestiones externas e internas pertinentes al SGSI;
- cambios en necesidades y expectativas de partes interesadas;
- información sobre el comportamiento de la SI:
 - no conformidades y acciones correctivas
 - seguimiento y resultados de las mediciones
 - resultados de auditorías
 - cumplimiento de los objetivos de SI
- comentarios de partes interesadas
- resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo
- oportunidades para la mejora continua

Revisión por la Dirección

SALIDAS

- Decisiones relacionadas con:
- oportunidades de mejora
 - Necesidades de cambios al SGSI

Debe ser efectuada al menos 1 vez por año

Capítulos de Requisitos:

4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Apoyo.
8. Operación.
9. Evaluación de desempeño

10. Mejora

10. Mejora

10.1 Mejora continua

La organización **debe** mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

¿Cómo?

ISO27001 establece herramientas para mantener y mejorar continuamente el SGSI. Entre ellas:

- Revisión por la Dirección
- Auditorías internas,
- Revisión de los riesgos determinados
- Evaluación de los controles establecidos
- Revisión de incidentes de seguridad
- Revisión de KPI y/o SLA establecidos
- Cumplimiento de proveedores de servicios.
- Otros...

10. Mejora

10.2 No conformidad y acciones correctivas

Cuando ocurra una no conformidad, la organización **debe**:

- a) reaccionar ante la no conformidad, y según sea aplicable:
 - 1) llevar a cabo acciones para controlarla y corregirla,
 - 2) hacer frente a las consecuencias;
- b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante:
 - 1) la revisión de la no conformidad,
 - 2) la determinación de las causas de la no conformidad, y
 - 3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;
- c) implementar cualquier acción necesaria;
- d) revisar la eficacia de las acciones correctivas llevadas a cabo; y
- e) si es necesario, hacer cambios al sistema de gestión de la seguridad de la información.

10. Mejora

10.2 No conformidad y acciones correctivas (continuación)

Las acciones correctivas **deben** ser adecuadas a los efectos de las no conformidades encontradas. La organización **debe** tener disponible **información documentada, como evidencia** de:



Evidencia
requerida

- f) la naturaleza de las no conformidades y cualquier acción posterior llevada a cabo;
- g) los resultados de cualquier acción correctiva.





fcfm

ESCUELA DE POSTGRADO
Y EDUCACIÓN CONTINUA
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

ISO 27001:2022

Interpretación de Requisitos