certiprof®

ISO 27001 LEAD IMPLEMENTER
PROFESSIONAL CERTIFICATION

I27001LI™ Versión 042024

ISO IEC 27001:2022 LEAD IMPLEMENTER CERTIFIED

I27001LI™ Versión 042024

¿Quién es Certiprof®?

Certiprof® es una entidad certificadora fundada en los Estados Unidos en 2015, ubicada actualmente en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **Nuestros Lifelong Learners (LLL)** se identifican como Aprendices Continuos, lo que demuestra su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digital en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- Las universidades, centros de formación, y facilitadores en todo el mundo forman parte de nuestra red de aliados **CPLS (Certified Partner For Learning Solutions).**
- **Los autores (co-creadores)** son expertos de la industria o practicantes que, con su conocimiento, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Personal Interno:** Nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos está a cargo de superar obstáculos, encontrar soluciones y entregar resultados excepcionales.

Nuestras Afiliaciones

Memberships

itcc
IT CERTIFICATION COUNCIL

Agile Alliance®

ANSI MEMBER

Digital badges issued by

Credly
by Pearson

IT Certification Council - ITCC

Certiprof® es un miembro activo de ITCC.

Una de las ventajas de hacer parte del ITCC es como líderes del sector colaboran entre sí en un formato abierto para explorar maneras nuevas o diferentes formas de hacer negocios que inspiran y fomentan la innovación, estableciendo y compartiendo buenas prácticas que nos permiten extender ese conocimiento a nuestra comunidad.

Certiprof ha contribuido a la elaboración de documentos blancos en el Career Path Ways Taskforce, un grupo de trabajo que se implementó internamente para ofrecer a los estudiantes la oportunidad de saber qué camino tomar después de una certificación.

Algunos de los miembros del ITCC

- **IBM**
- **CISCO**
- **ADOBE**
- **AWS**
- **SAP**
- **GOOGLE**
- **ISACA**

Agile Alliance

Certiprof® es un miembro corporativo de Agile Alliance.

Al unirnos al programa corporativo Agile Alliance, continuamos empoderando a las personas ayudándolas a alcanzar su potencial a través de la educación. Cada día, brindamos más herramientas y recursos que permiten a nuestros socios formar profesionales que buscan mejorar su desarrollo profesional y sus habilidades.

https://www.agilealliance.org/organizations/certiprof/

Credly

Esta alianza permite que las personas y empresas certificadas con Certiprof® cuenten con una distinción a nivel mundial a través de un distintivo digital.

Credly es el emisor de insignias más importante del mundo y empresas líderes en tecnología como IBM, Microsoft, PMI,Nokia, la Universidad de Stanford, entre otras, emiten sus insignias con Credly.

Empresas que emiten insignias de validación de conocimiento con Credly:

- **IBM**
- **Microsoft**
- **PMI**
- **Universidad de Stanford**
- **Certiprof**

Insignias Digitales

Insignias Digitales:
¿Qué Son?

Según el estudio del IT Certification Council (ITCC), años atrás, la gente sabía muy poco sobre las insignias digitales. Hoy, grandes empresas e instituciones educativas de todo el mundo expiden insignias.

Las insignias digitales contienen metadatos detallados sobre quién las ha obtenido, las competencias requeridas y la organización que las ha expedido. Algunas insignias incluso están vinculadas a las actividades necesarias para obtenerlas.

Para las empresas e instituciones educativas, las insignias y la información que proporcionan son tan importantes que muchas decisiones, como las de contratación o admisión, se basan en los datos que aportan.

¿Por qué son importantes?

- **Facilidad de Compartir y Verificar Logros:**

  Las insignias digitales permiten a los profesionales mostrar y verificar sus logros de manera instantánea y global. Según un informe de Credly, **los perfiles de LinkedIn con insignias digitales reciben un 40% más de atención por parte de reclutadores y empleadores.**

- **Visibilidad en Plataformas Digitales:**

  En una encuesta realizada por Pearson y Credly, el **85%** de los usuarios que obtuvieron insignias digitales **las compartieron en LinkedIn,** y el **75%** reportó que esto mejoró su **credibilidad profesional en sus redes.** Además, el **76%** de los empleadores encuestados afirmó que las insignias digitales les ayudan a identificar rápidamente habilidades específicas.

¿Por qué son importantes?

- **Impacto en la Contratación:**

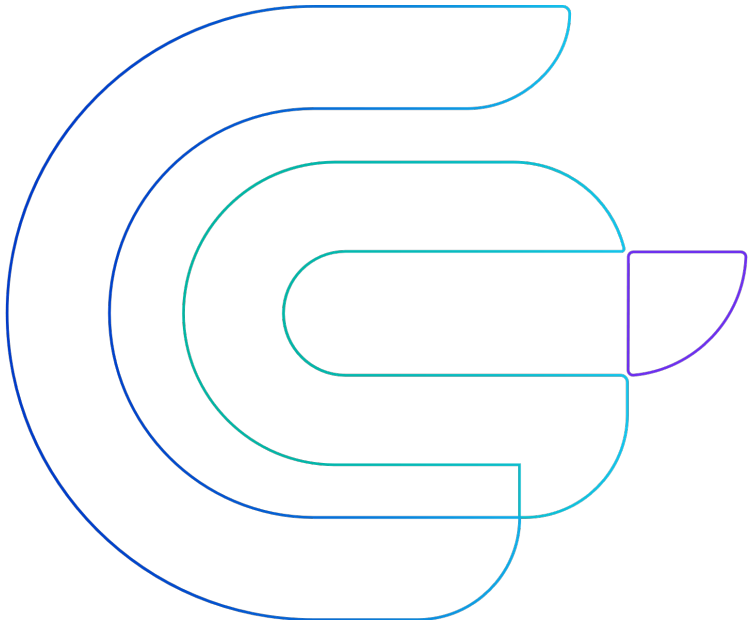
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿Por qué son importantes?

- **Empoderamiento de la Marca Personal:**

La visibilidad y verificación instantánea proporcionada por las insignias digitales permiten a los profesionales no solo demostrar sus habilidades, sino también construir una marca personal fuerte. Según un estudio de LinkedIn, los profesionales que utilizan insignias digitales tienen un 24% más de probabilidades de avanzar en sus carreras.

La certificación y las insignias digitales no son solo una validación del conocimiento, sino también una herramienta poderosa para la mejora continua y la empleabilidad. En un mundo donde el aprendizaje permanente se ha convertido en la norma, estas credenciales son clave para el desarrollo profesional y la competitividad en el mercado laboral global.



No todas las insignias son iguales, y en **Certiprof,** estamos comprometidos con ofrecerte más que un simple reconocimiento digital. Al obtener una insignia emitida por certiprof, estarás recibiendo una validación de tu conocimiento respaldada por una de las entidades líderes en certificación profesional a nivel mundial.

Da el siguiente paso y obtén la insignia que te abrirá puertas y te posicionará como un experto en tu campo.

¿Por qué es importante obtener su certificado?

- **Prueba de experiencia:** Su certificado es un reconocimiento formal de las habilidades y conocimientos que ha adquirido. Sirve como prueba verificable de sus cualificaciones y demuestra su compromiso con la excelencia en su campo.

- **Credibilidad y reconocimiento:** En el competitivo mercado laboral actual, las empresas y los compañeros valoran las credenciales que le distinguen de los demás. Un certificado de una institución reconocida, como Certiprof, proporciona credibilidad instantánea e impulsa su reputación profesional.

- **Avance profesional:** Tener tu certificado puede abrirte las puertas a nuevas oportunidades. Ya se trate de un ascenso, un aumento de sueldo o un nuevo puesto de trabajo, las certificaciones son un factor diferenciador clave que los empleadores tienen en cuenta a la hora de evaluar a los candidatos.

¿Por qué es importante obtener su certificado?

- **Oportunidades de establecer contactos:** Poseer un certificado le conecta con una red de profesionales certificados. Muchas organizaciones cuentan con grupos de antiguos alumnos o de trabajo en red en los que puede compartir experiencias, intercambiar ideas y ampliar su círculo profesional.

- **Logro personal:** Obtener una certificación es un logro importante, y su certificado es un recordatorio tangible del trabajo duro, la dedicación y el progreso que ha realizado. Es algo de lo que puede sentirse orgulloso y mostrar a los demás.

Insignia

ISO 27001 Certified Lead Implementer - I27001LI

Issued by Certiprof

Holders of this certification have demonstrated an understanding of implementing a comprehensive management system, based on an enterprise risk approach to establish, implement, operate, monitor, review, maintain and improve information security. Furthermore, they have the skills to define business cases, GAP Analysis and the ability to plan and take action to address risks and opportunities.

Learn more

Earn this Badge

Certification Paid

Skills

Analysing Data Protection Risk | Basic Information Security Management (ISMS) Require... | Building A Business Case | Continual Improvement | Risk Management

https://www.credly.com/org/certiprof/badge/iso-27001-certified-lead-implementer-i27001li

Aprendizaje Permanente

- Certiprof ha creado una insignia especial para reconocer a los aprendices constantes.
- Para el 2024, se han emitido más de 1,000,000 de estas insignias en más de 11 idiomas.

Propósito y Filosofía

- Esta insignia está destinada a personas que creen firmemente en que la educación puede cambiar vidas y transformar el mundo.
- La filosofía detrás de la insignia es promover el compromiso con el aprendizaje continuo a lo largo de la vida.

Acceso y Obtención de la Insignia

- La insignia de Lifelong Learning se entrega sin costo a aquellos que se identifican con este enfoque de aprendizaje.
- Cualquier persona que se considere un aprendiz constante puede reclamar su insignia visitando:

https://certiprof.com/pages/certiprof-lifelong-learning

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#I27001LI #certiprof

certiprof®

Agenda

1) Introducción a los sistemas de gestión.
2) Pasos generales en la Implementación.
3) Caso de negocio, análisis GAP y plan de acción.

4)Interpretar los requisitos de las cláusulas de cumplimiento (4 a 10) ISO IEC 27001.

- Cláusula 4 Contexto de la Organización.
  - Metodología: Alcance y Límite del SGSI.
- Cláusula 5 Liderazgo.
  - Metodología: Política del SGSI.
- Cláusula 6 Planificación.
  - Metodología: Proceso de Gestión de Riesgos.
- Cláusula 7 Soporte.
- Cláusula 8 Operación.
- Cláusula 9 Evaluación del Desempeño.
  - Metodología: Auditoria interna.
- Cláusula 10 Mejora.

1. Introducción a los Sistemas de Gestión

1.1 Información y principios generales.
1.2 La Seguridad de la Información.
1.3 El sistema de Gestión de la Seguridad de la Información – SGSI.
1.4 Factores Críticos de Éxito de un SGSI.
1.5 Beneficios de un SGSI.
1.6 Estructura de la ISO IEC 27001:2022.
1.7 ISO 27002:2022.

Objetivo del Módulo

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder obtendrá conocimientos básicos sobre un SGSI y la estructura de la norma ISO IEC 27001:2022.

1.1 Información y Principios Generales

Un **SGSI** (*Sistema de Gestión de la Seguridad de la Información*) consiste en un conjunto de políticas, procedimientos, Guías, recursos y actividades asociadas, que son gestionados de manera colectiva por una organización.

Un **SGSI** es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

El SGSI se conecta con la ISO 27005 como familia, la cual desarrolla una visión del proceso del riesgo de seguridad en la información con: Establecimiento de contexto, identificación, estimación evaluación, tratamiento y aceptación del riesgo de la organización.

El SGSI protege los activos de la información y contiene los controles adecuados para garantizar la protección de estos activos de información.

1.1 Información y Principios Generales

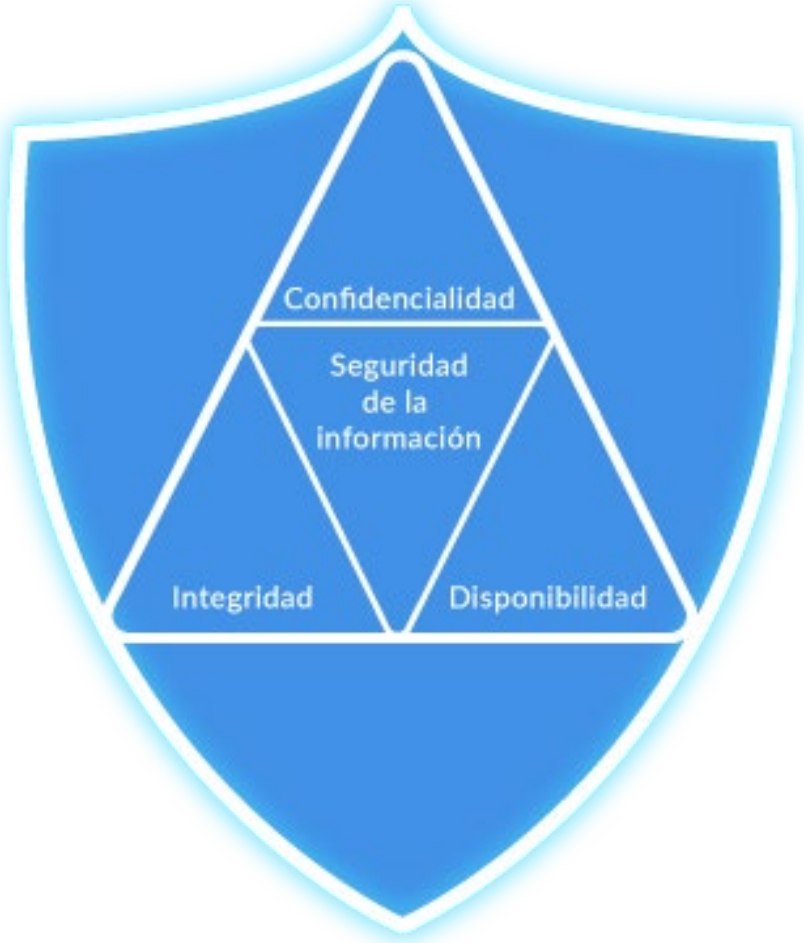
Contribución a la Organización de un **SGSI**:

a) La conciencia de la Organización en la necesidad de seguridad de la información
b) La asignación de responsabilidades en seguridad de la información
c) El compromiso de la Alta Dirección
d) Tomar en cuenta la necesidad y requisitos de las partes interesadas
e) La gestión de los riesgo para determinar los controles adecuados para alcanzar niveles aceptables de riesgo
f) La seguridad de la información como un componente esencial de los procesos
g) La prevención y detección activas de incidentes de seguridad de la información
h) Generación de capacidad de cumplimiento
i) La mejora continua de los procesos a través de la seguridad de la información

1.2 La Seguridad de la Información

Define tres dimensiones principales: **la confidencialidad**, **la disponibilidad** y **la integridad**.

- **Disponibilidad** Propiedad que la información sea accesible y utilizable por solicitud de los autorizados 2.10 ISO 27000
- **Confidencialidad** Propiedad que determina que la información no está disponible ni sea revelada a quien no esté autorizado 2.13 ISO 27000
- **Integridad** Propiedad de salvaguardar la exactitud y el estado completo de los activos 2.36 ISO 27000



1.2 La Seguridad de la Información

La seguridad de la información se consigue mediante la implementación de un conjunto de requisitos y controles aplicables, seleccionados a través del proceso de gestión de riesgo por medio de un **SGSI**, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

Estos controles necesitan ser especificados, implementados, monitoreados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de negocio de una organización.

1.3 El Sistema de Gestión de Seguridad de la Información (SGSI)

Un sistema de gestión utiliza un marco de recursos para alcanzar los objetos de una organización. El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

En términos de seguridad de la información, un sistema de gestión permite a una organización:

a) Satisfacer los requisitos de seguridad de los clientes y otras partes interesadas
b) Mejorar los planes y actividades de la organización
c) Cumplir con los objetivos de seguridad de información de la organización
d) Cumplir con las regulaciones, leyes y obligaciones sectoriales
e) Gestionar los activos de información de una manera organizada que facilita la mejora continua y la adaptación a las actuales metas de la organización y a su entorno

1.4 Factores críticos de éxito de un SGSI

Un gran número de factores son fundamentales para la implementación exitosa de un **SGSI** que permite a una organización cumplir con sus objetivos de negocio. Algunos ejemplos de factores críticos de éxito son:

a) Que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos del negocio
b) Un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia de la cultura de la organización
c) El apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de alta Dirección
d) El conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información (véase la Norma ISO IEC 27005)

1.4 Factores críticos de éxito de un SGSI

e) Un programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes interesadas de sus responsabilidades en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc
f) Un proceso eficaz de gestión de incidentes de seguridad de la información
g) Un enfoque efectivo de gestión de la continuidad del negocio
h) Un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora

Un **SGSI** aumenta la probabilidad de que una organización alcance de forma coherente los factores críticos de éxito para proteger sus activos de información.

1.5 Beneficios de un SGSI

Los beneficios de implementar un **SGSI** producirán principalmente una reducción de los riesgos asociados a la seguridad de la información contribuyendo en:

a) Una ayuda para la dirección en la estructura de su enfoque hacia la gestión de la seguridad de la información
b) Un gobierno del riesgo corporativo, acciones de educación y formación en la gestión de la seguridad de la información
c) La promoción de buenas prácticas de seguridad de la información, aceptadas a nivel mundial
d) Disponer de un lenguaje común para la seguridad de la información
e) Lograr competitividad con la certificación de la Norma ISO IEC 27001 por un organismo de certificación acreditado
f) Aumentar la confianza en la organización por las partes interesadas
g) Eficaz gestión de las inversiones en seguridad de la información

1.6 Estructura de la ISO IEC 27001:2022 (Familia)

1.6 Estructura de la ISO IEC 27001:2022

ISO IEC 27001:2022

Cláusulas

1. OBJETO Y CAMPO DE APLICACIÓN
2. REFERENCIAS NORMATIVAS
3. TÉRMINOS Y DEFINICIONES
4. CONTEXTO DE LA ORGANIZACIÓN
5. LIDERAZGO
6. PLANIFICACIÓN
7. SOPORTE
8. OPERACIÓN
9. EVALUACIÓN DEL DESEMPEÑO
10. MEJORA

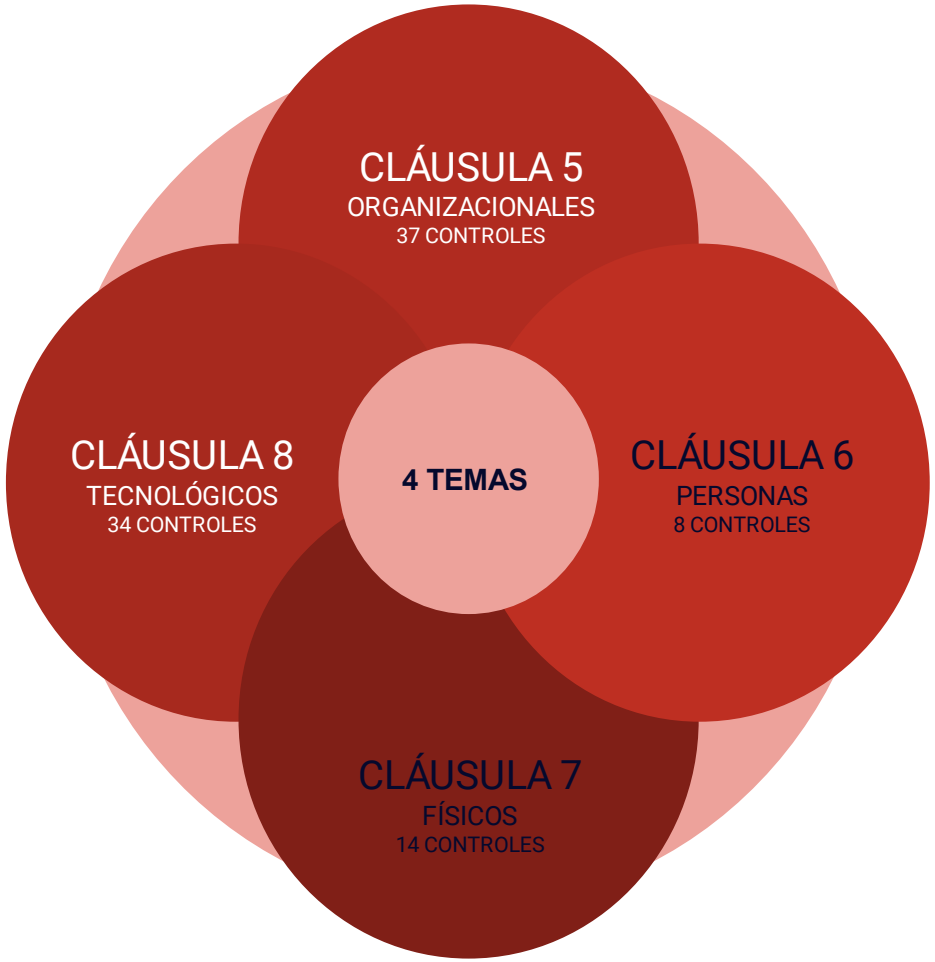
ESTRUCTURA DE ALTO NIVEL

- La adopción de un lenguaje simple que facilita que las empresas integren diferentes Sistemas de Gestión.
- Un enunciado idéntico para requisitos idénticos.

Anexo SL

1.6 Estructura del Anexo A

Categorización Anexo A



1.7 ISO 27002:2022

Este documento proporciona un conjunto de referencia de controles genéricos de seguridad de la información, incluida una **Guía**. Este documento está diseñado para ser utilizado por organizaciones:

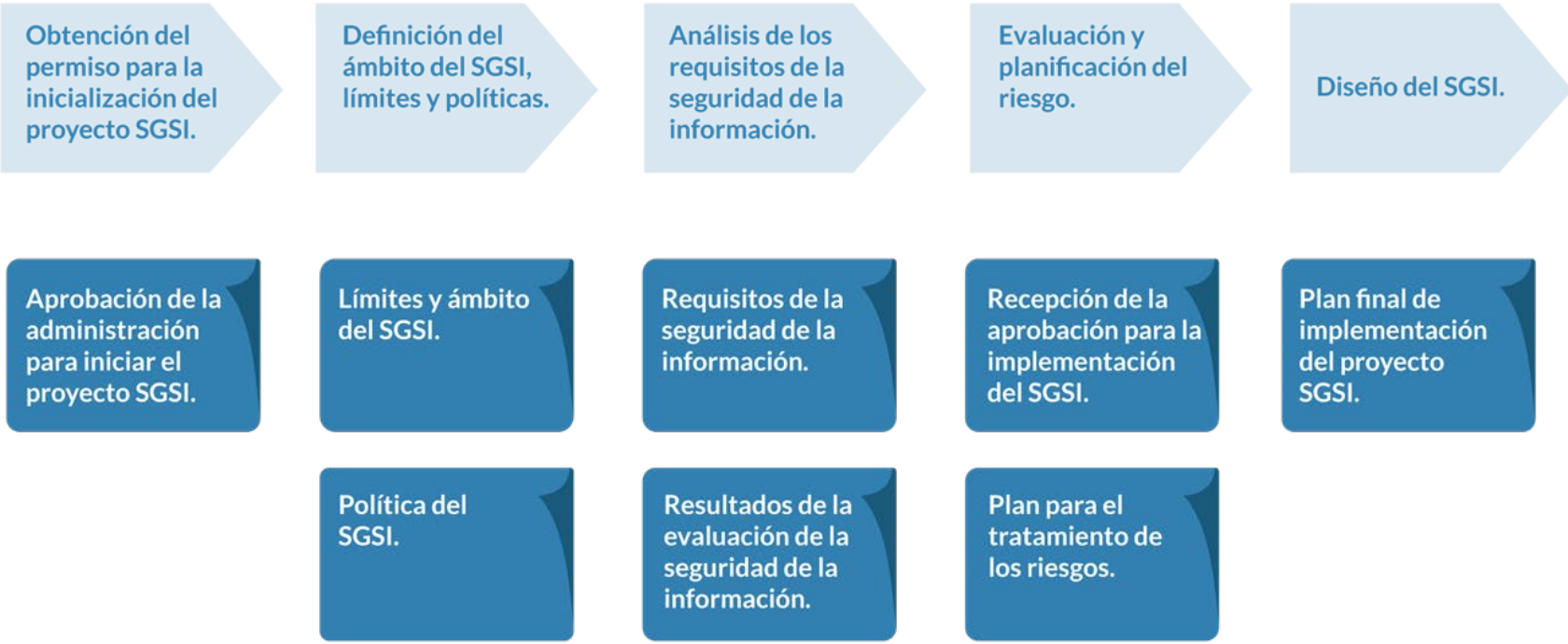
a) Dentro del contexto de un sistema de gestión de seguridad de la información (SGSI) basado en ISO IEC 27001;
b) Para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente;
c) Para desarrollar directrices de gestión de la seguridad de la información específicas de la organización

2. Pasos Generales en la Implementación

2.1 Ruta de navegación.
2.2 Ciclo Deming PHVA e ISO IEC 27001:2022.
2.3 PHVA Aplicado a la Implementación del SGSI
2.4 Etapas de Implementación de un SGSI.
2.5 Pasos Generales en la Implementación.
2.6 Vista General Final.

Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe entender la ruta (pasos) generales de una implementación del ISMS.



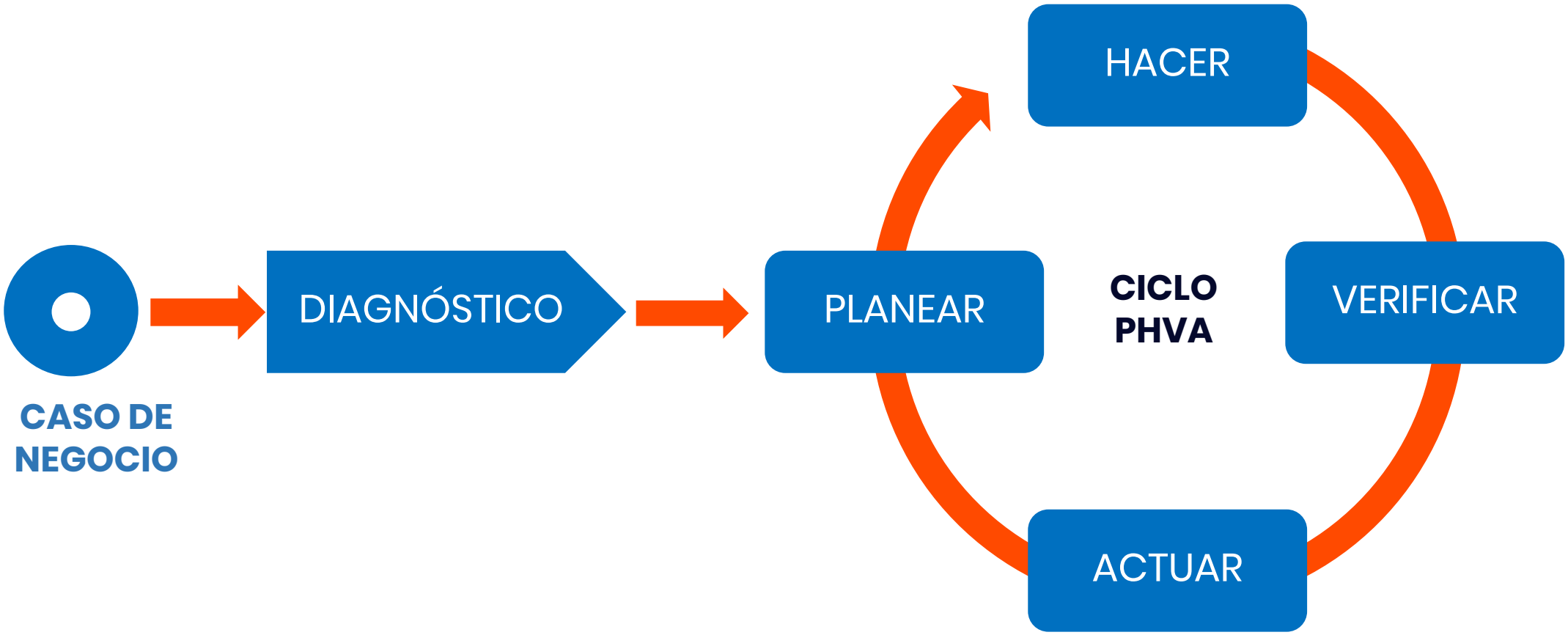
File:ISO27003.png - Wikimedia Commons. (2022). Retrieved 9 May 2022, from https://commons.wikimedia.org/wiki/File:ISO27003.png

IDENTIFICAR LAS FASES Y ACTIVIDADES DE UN PLAN DE IMPLEMENTACIÓN DE UN SGSI DE ACUERDO CON ISO 27003

	ACTIVIDADES
1	IDENTIFICAR LÓGICAMENTE FASES DEL PROYECTO DE IMPLEMENTACIÓN DE UN SGSI SEGÚN ISO IEC 27003
2	IDENTIFICAR, ANALIZAR, ESTABLECER E IMPLEMENTAR LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN.
3	DESARROLLAR LOS CONTROLES PROPUESTOS EN EL ANEXO A. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA.
4	ELABORAR EL DISEÑO DE UN SGSI

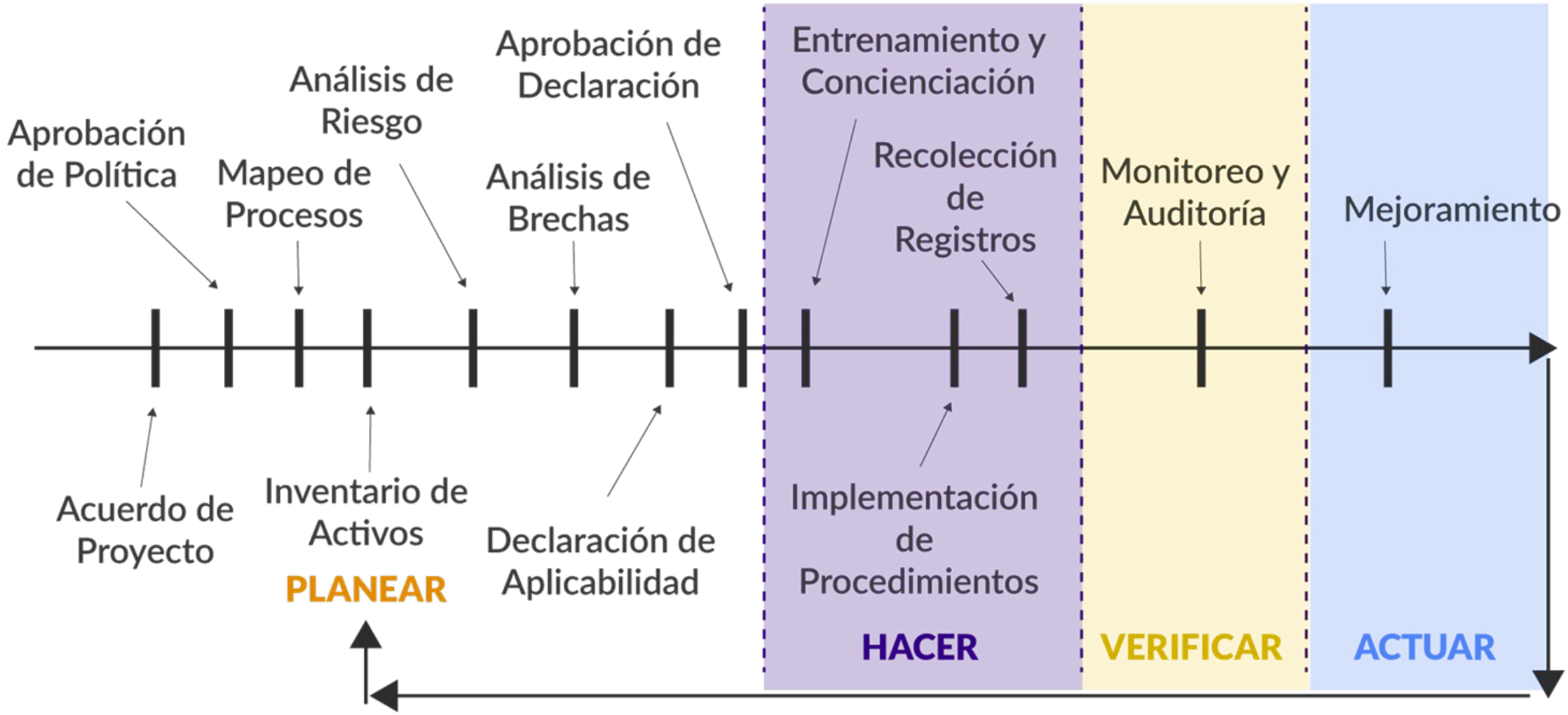
NOTA: El auditor valida que estos ciclos se cumplan con el fin de generar confianza para que las actividades de implementación se hayan cumplido. Existe la Guía DE UN SGSI (ISO IEC 27003).

2.1 Ruta de Navegación

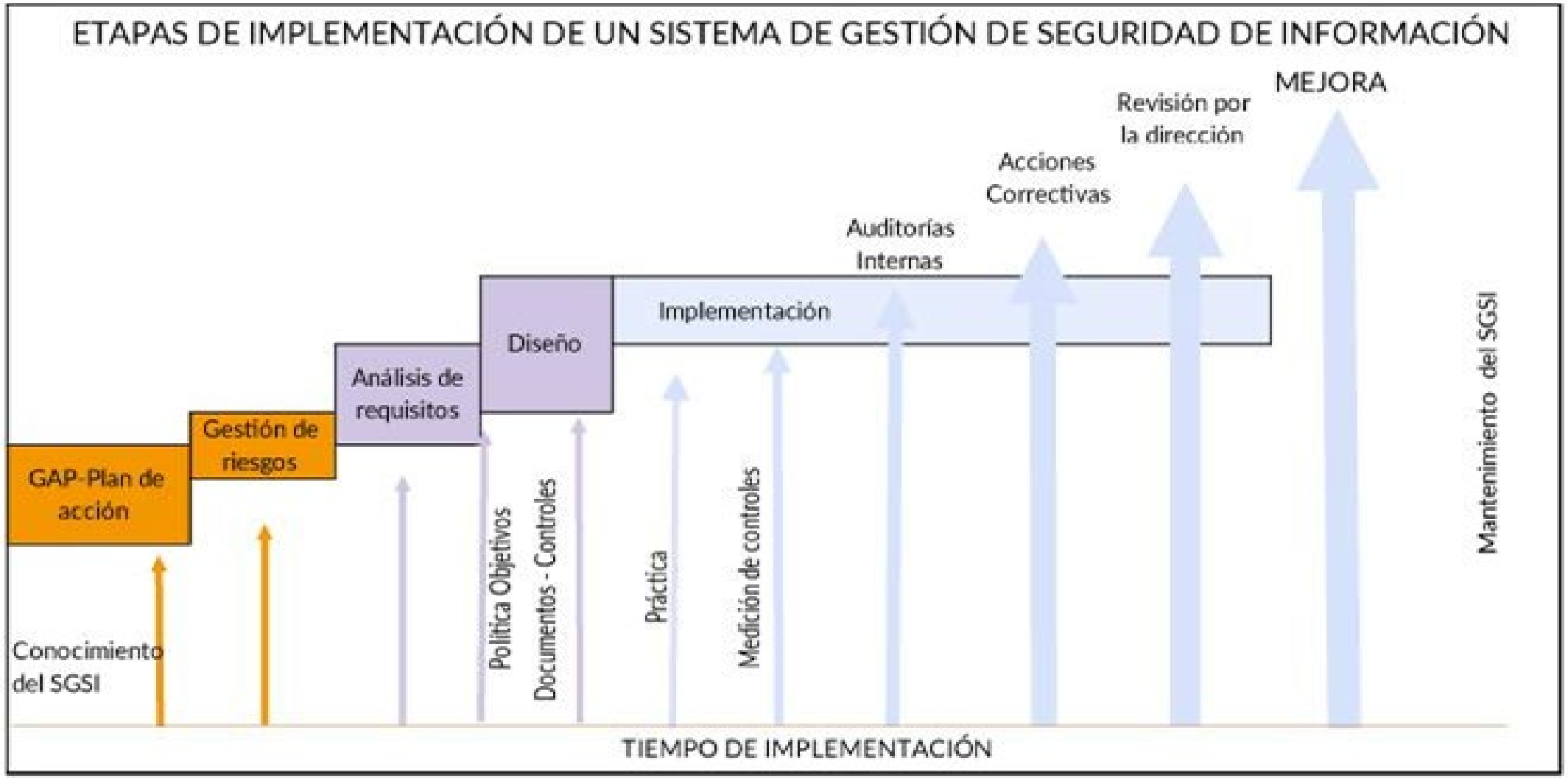


2.2 Ciclo Deming PHVA e ISO IEC 27001:2022

2.3 PHVA Aplicado a la Implementación del SGSI



2.4 Etapas de Implementación de un SGSI

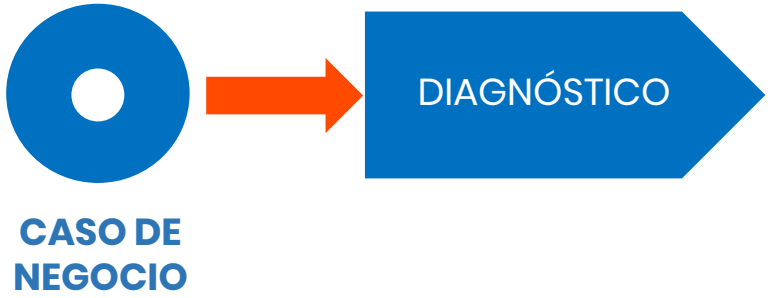


2.5 Pasos Generales en la Implementación

1. Respaldo de la dirección
   Caso de Negocio

2. Identificar Requisitos.
   Análisis del existente sistema, diagnóstico (Análisis GAP).

3. Creación del proyecto .
   Plan del Proyecto (Plan de acción).



4. Alcance y Objetivo de la dirección.
   Alcance del SGSI, objetivos.

5. Creación de la política de seguridad de la información.
   Política SGSI.

6. Proceso de riesgos.
   Metodología evaluación de riesgos.

7. Evaluación y tratamiento de riesgos.
   Informe evaluación de riesgos.

2.5 Pasos Generales en la Implementación

8. Definición de controles a implementar.
Declaración de aplicabilidad (SoA).

9. Quién implementará los controles.
Tratamiento del riesgo, Planificación.

10. Medición de la efectividad.
Metodología de medición.

11. Implementar controles y procedimientos de apoyo.

12. Implementar programas de capacitación y concienciación.

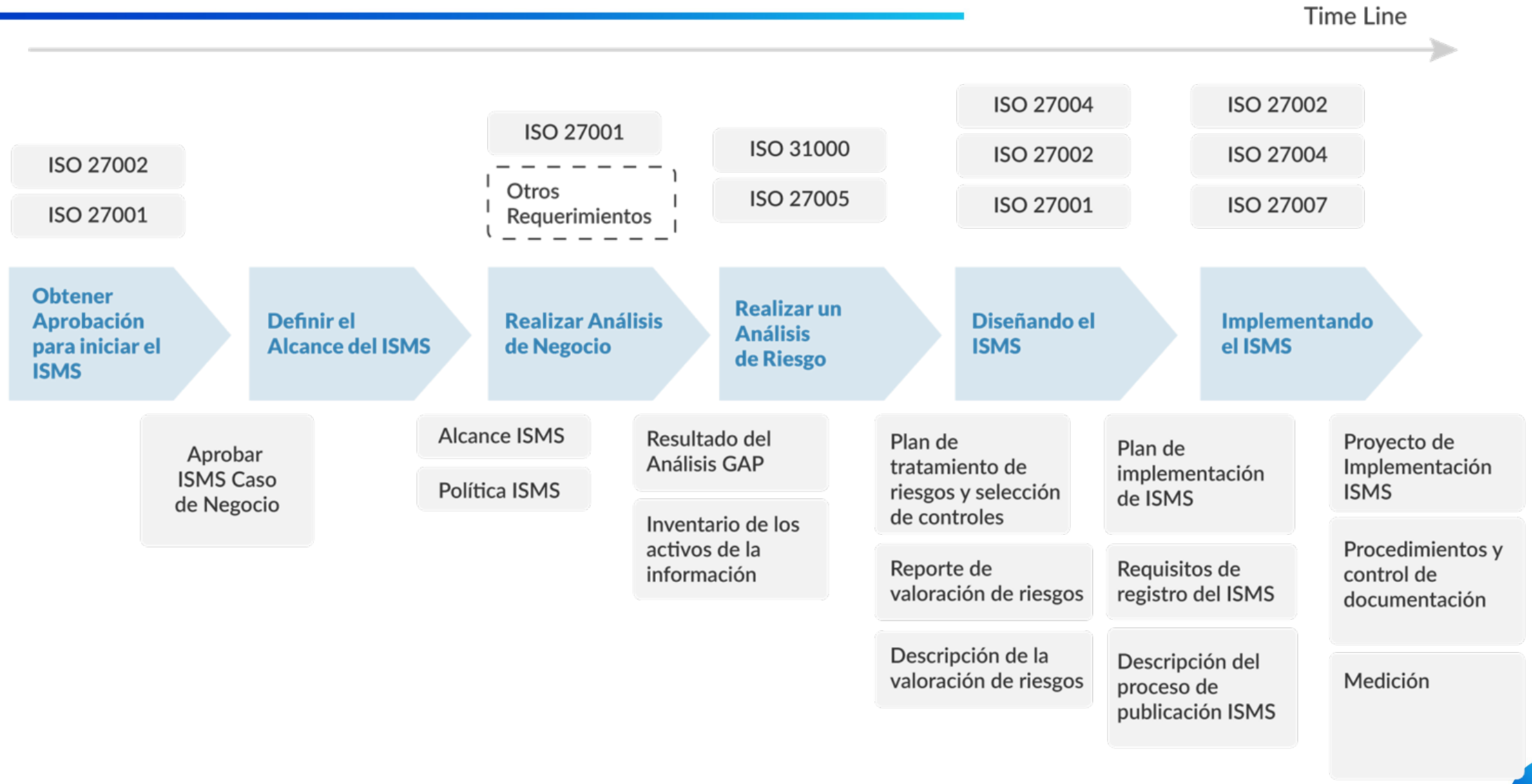
13. Supervisión del SGSI.
Registros.

14. Auditoría interna.
Informes de Auditoría, medidas correctivas.

15. Revisión por parte de la dirección.

16. Mejora continua.
Metodologías y marcos de mejora.

2.6 Vista General Final

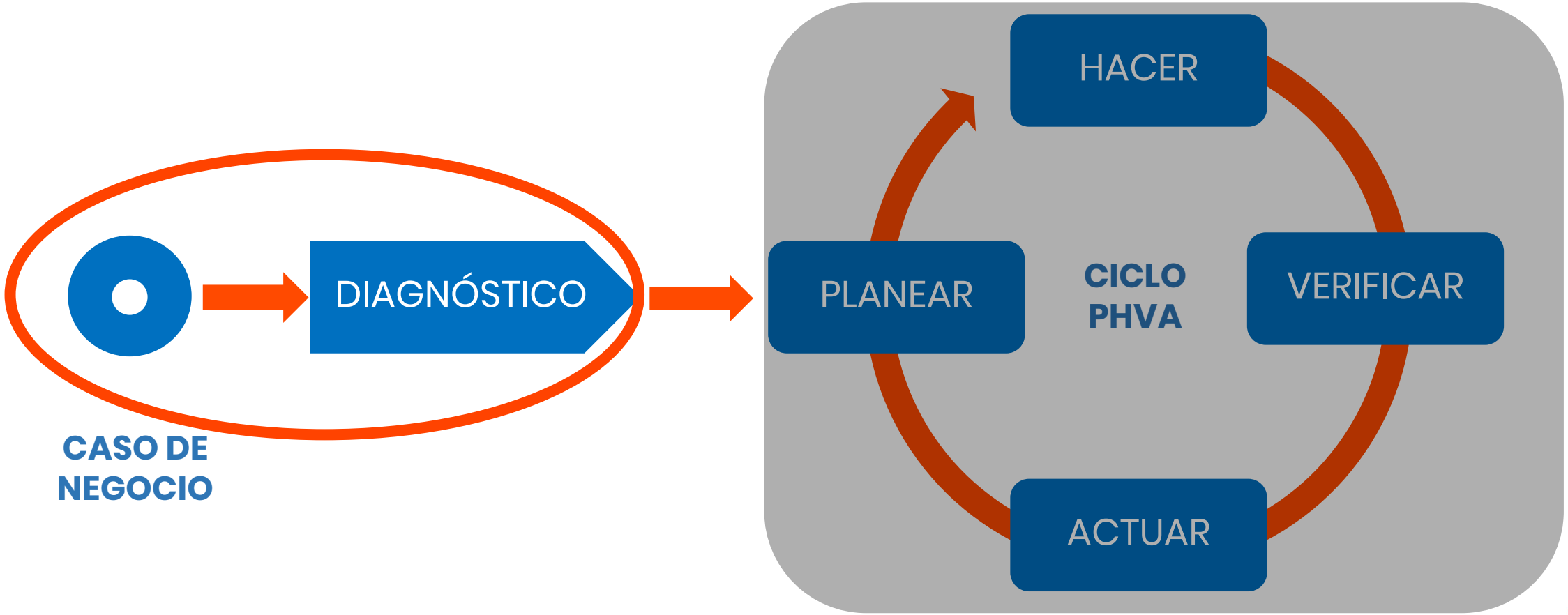


3. Caso de negocio, Análisis GAP y plan de acción

3.1 Caso de negocio.
3.2 Partes de un Caso de Negocio.
3.3 Análisis de Brechas - Análisis GAP.
3.4 Objetivos Análisis GAP.
3.5 Modelos de Madurez.
3.6 Cómo Realizar un Análisis de Brechas GAP.
3.7 Modelo de Madurez COBIT.
3.9 Visión de Proyecto y plan de acción.

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la primera fase (caso de negocio y diagnóstico) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



3.1 Caso de Negocio

"Un documento la define la propuesta, plantea sus objetivos, productos por entregar, el costo y esfuerzo estimados y el alcance".

Tom Mochal

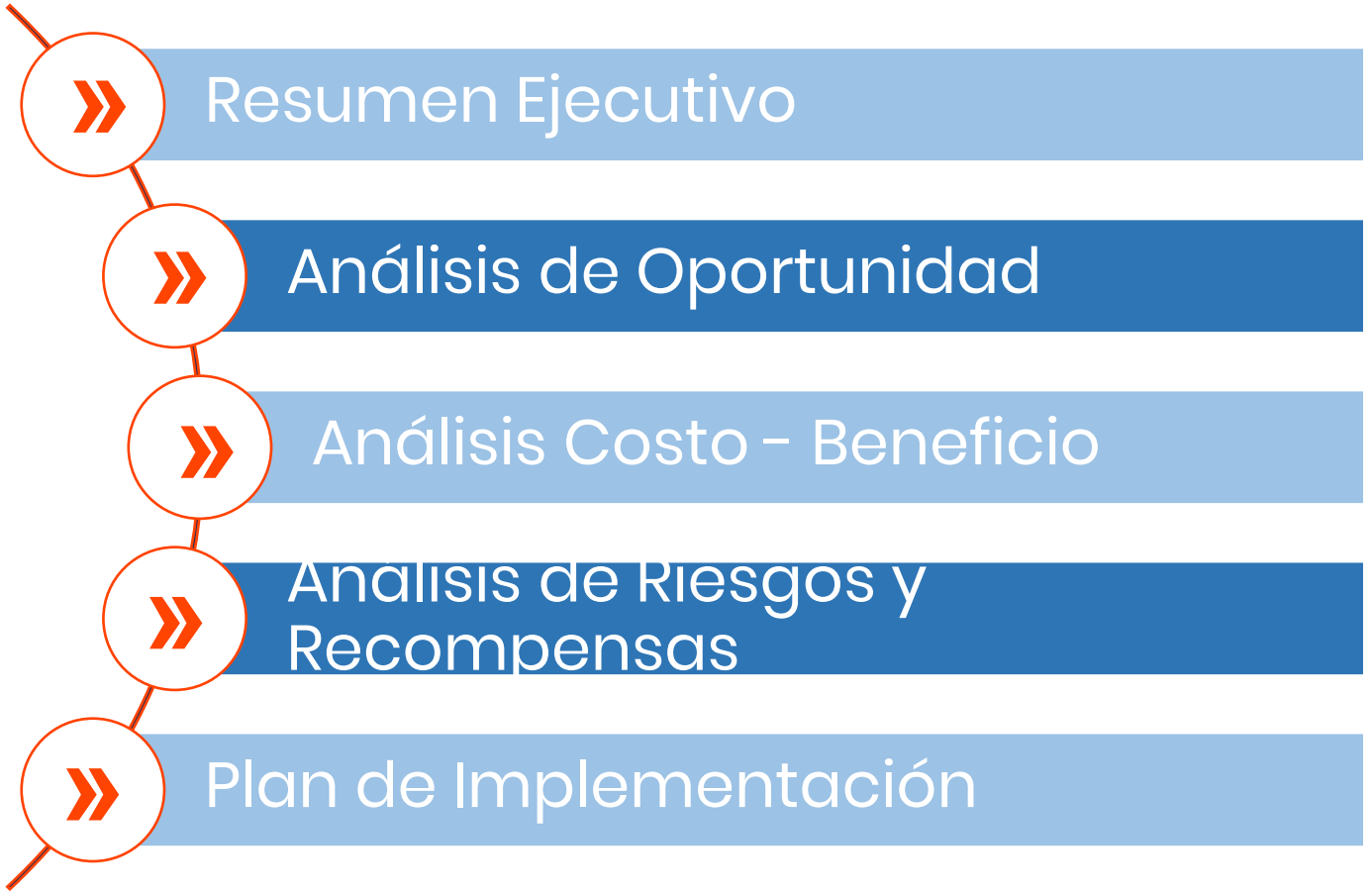
Fuente: *Tom Mochal, "Select and prioritize projects with a business case", Diciembre 15, 2003. (Véase: https://www.techrepublic.com/article/select-and-prioritize-projects-with-a-business-case/).*

3.1 Caso de Negocio

Documento que resume a la **Alta Dirección** los principales aspectos a tener en cuenta para implantar un Sistema de gestión de la Seguridad de la Información (SGSI).

3.2 Partes de un Caso de Negocio

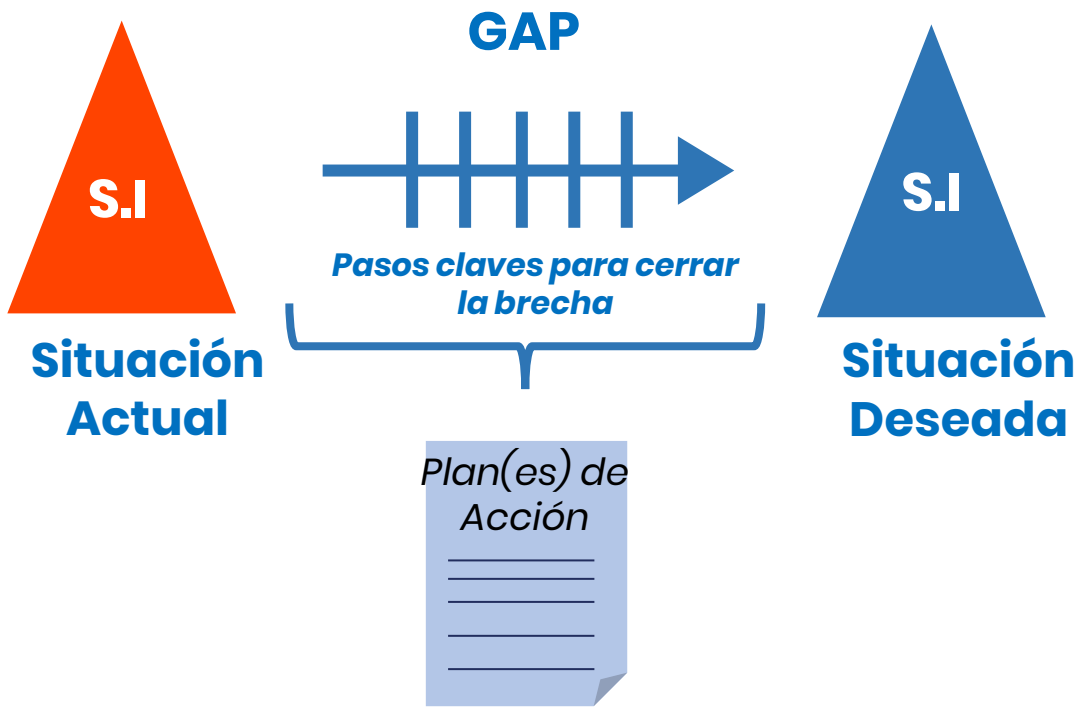
Partes de un Caso de Negocio



3.2 Partes de un Caso de Negocio

Resumen Ejecutivo	• Descripción del problema del negocio que el proyecto solucionará • Cómo el proyecto beneficiará al negocio • Cómo el proyecto se alinea con las necesidades estratégicas de la organización
Análisis de Oportunidad	• Contexto organizacional interno y externo en términos de SI • Principales Necesidades de las partes interesadas • Necesidades Relevantes frente a temas legales, según el sector
Análisis Costo - Beneficio	• Detallar la descripción general de costos y beneficios (Cuantificables) • Retorno de la inversión • Plantear escenarios
Análisis Riesgo y Recompensas	• Riesgos externos e internos más relevantes en el sector por las cuales se debería implementar un SGSI y cuál es el costo probable si se llegan a materializar
Plan de Implementación	• Actividades, tiempos, recursos, metas (Mediciones en cumplimiento, calidad de avance y Presupuesto)

3.3 Análisis de Brechas – Análisis GAP



Un análisis de brechas GAP o análisis de deficiencias consiste en un análisis de **cumplimiento** tanto con los **requisitos** de la norma ISO IEC 27001:2022 como de sus **controles** (Anexo A).

Un análisis GAP nos brinda el estado actual y permite determinar el plan necesario para cerrar las brechas. (*También conocido como plan de acción*).

Un análisis de brechas ISO IEC 27001:2022, también conocido a veces como evaluación de cumplimiento o evaluación previa, es una evaluación que proporciona una descripción general de alto nivel de la postura de seguridad actual de su organización.

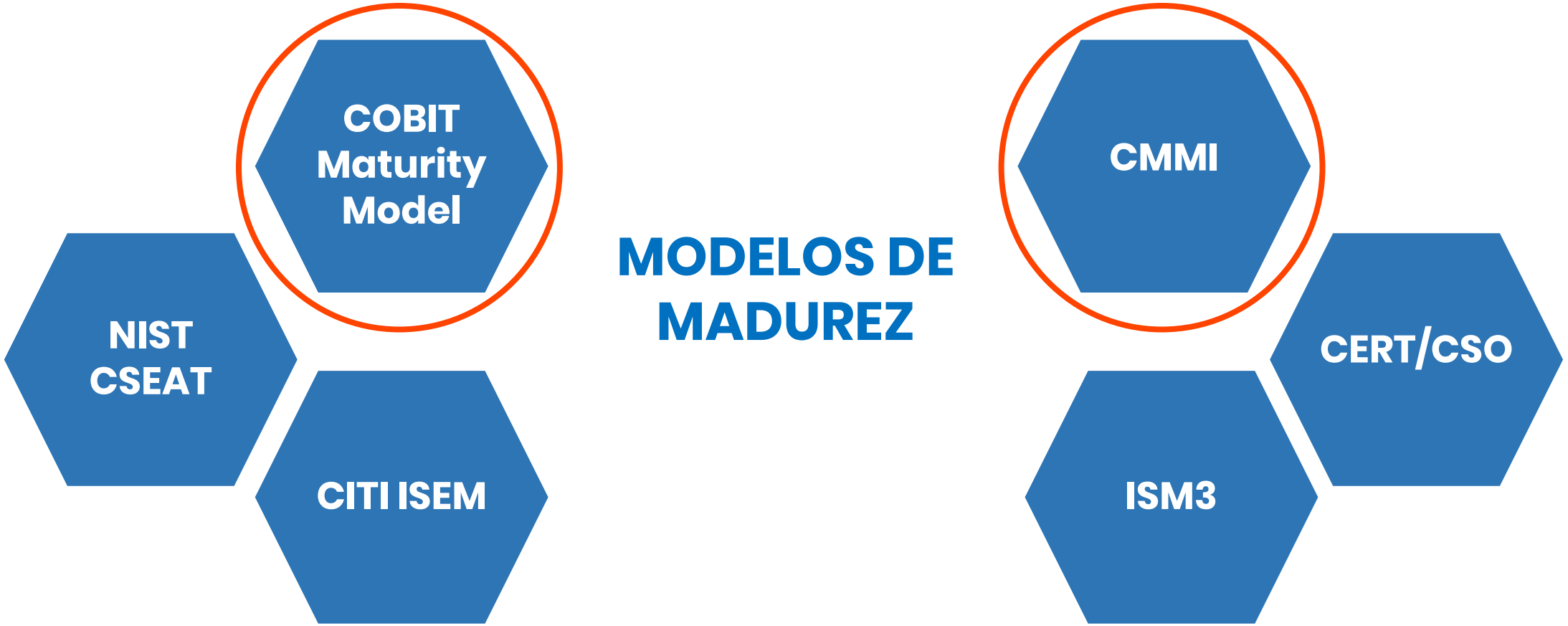
3.4 Objetivos Análisis GAP

OBJETIVOS ANÁLISIS GAP

Establecer el punto de partida para implementar la norma y evaluar el esfuerzo necesario así como tener una herramienta fiable para elaborar un plan de implementación de ISO IEC 27001:2022.

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.

3.5 Modelos de Madurez



3.6 Cómo Realizar un Análisis de Brechas GAP

Para la realización del análisis de deficiencias GAP puede ser aconsejable utilizar **un modelo de madurez** para la evaluación del cumplimiento.

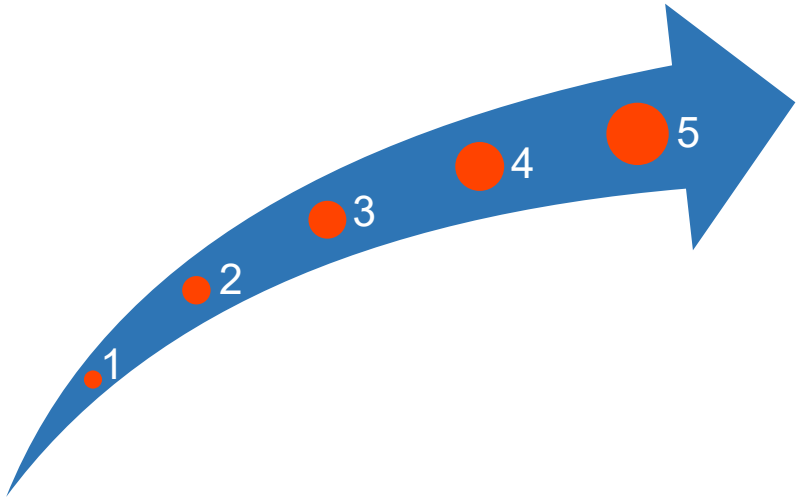
¿Qué es un modelo de madurez?

Es un conjunto y estructura de elementos que describen el nivel de madurez de un ente en un aspecto determinado, cada modelo propone una escala de madurez ó cumplimiento de 4, 5 o 6 niveles

¿Para qué sirve?

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

3.6 Cómo Realizar un Análisis de Brechas GAP



Para establecer el nivel de madurez actual para cada uno de los requisitos y controles de la ISO IEC 27001 se realiza una serie de preguntas (test de cumplimiento), el resultado de esta evaluación posicionará a la organización dentro de una escala según el modelo de madurez definido.

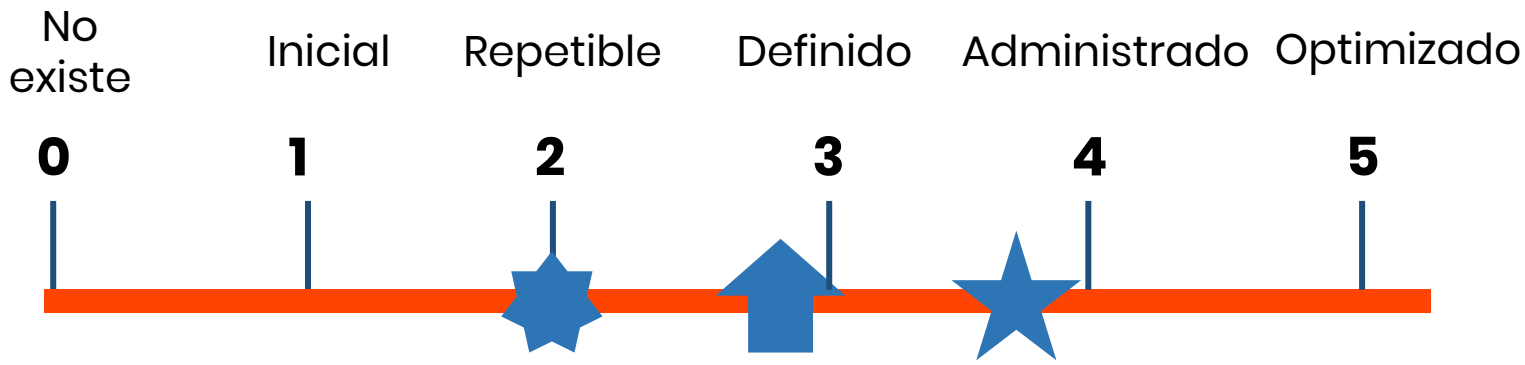
El test de cumplimiento puede ser una lista de preguntas bajo diferentes escenarios de acuerdo al modelo de madurez definido, diseñando cuidadosamente las preguntas usando la norma ISO27001:2022 y su ANEXO A.

TEST CUMPLIMIENTO 27001:2022

TEST CUMPLIMIENTO ANEXO A 27001:2022

3.7 Modelo de Madurez COBIT

Tomando como ejemplo el modelo de madurez COBIT, este nos permite evaluar el nivel de madurez actual respecto a los **requisitos** (Numerales) y **controles** (Anexo A) de la ISO IEC 27001 en una escala de 5 niveles:



Símbolos Utilizados

- Estado actual de la empresa
- Promedio de la industria
- Objetivo de la empresa

Calificativos Utilizados

0. No se aplica la administración de procesos.
1. Los procesos son ad-hoc y desorganizados.
2. Los procesos siguen un patrón regular.
3. Los procesos se documentan y se comunican.
4. Los procesos se monitorean y miden.
5. Se utilizan buenas prácticas y están automatizadas.

3.9 Visión de Proyecto y plan de acción

Una vez concluido el análisis GAP podemos contar con un plan de acción para iniciar con la implementación del SGSI.

La implementación del Sistema debe ser vista como un proyecto inicialmente que después debe ser mantenido y mejorado en la operación.

El plan de acción puede contener:

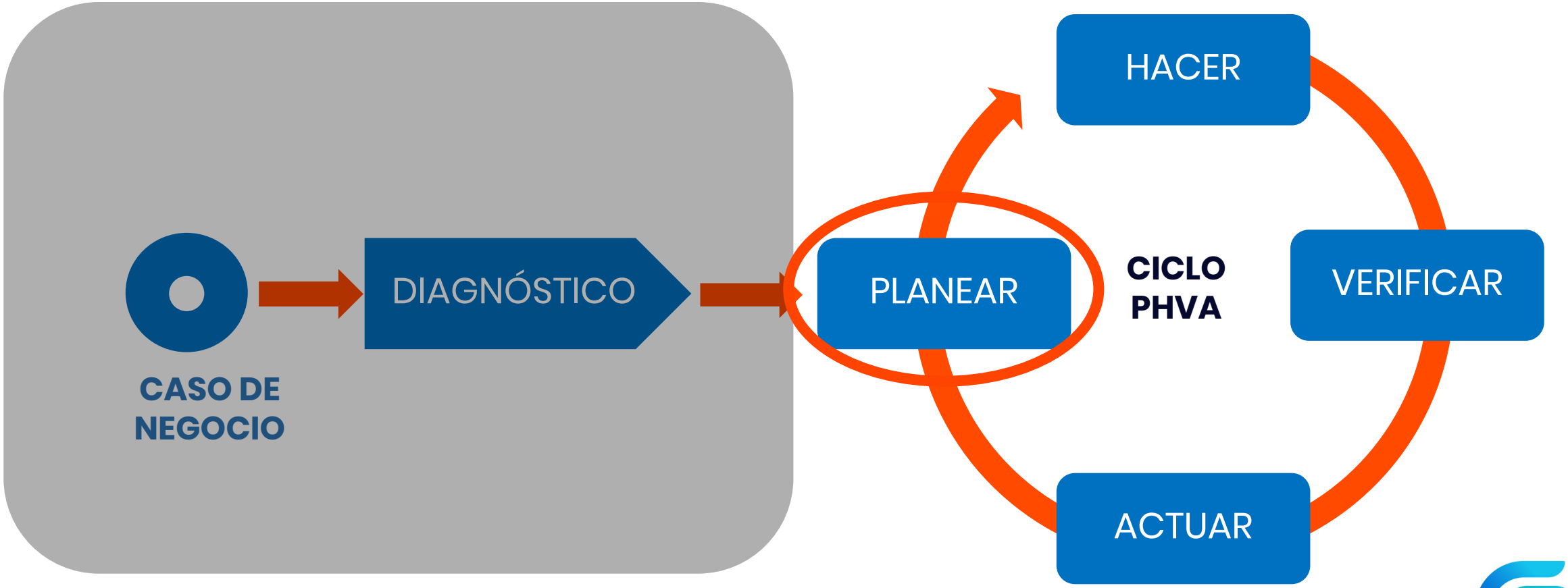
- Objetivo, alcance y usuarios.
- Documentos de referencia.
- Proyecto de implementación del SGSI.
- Objetivo del proyecto.
- Resultados del proyecto.
- Cronograma.
- Organización del proyecto.
  - Patrocinado del proyecto.
  - Gerente del proyecto.
  - Equipo del proyecto.
- Principales riesgos del plan.
- Herramientas para implementación del proyecto y generación de informes.
- Gestión de registros.
- Validez y gestión de documentos.

4. Contexto de la Organización: Interpretar los Requisitos ISO IEC 27001

4.1 Comprensión de la Organización y su Contexto.
4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas.
4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información.
4.4 Sistema de seguridad de la información.

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (Planear) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de diseñar el **alcance del ISMS.**

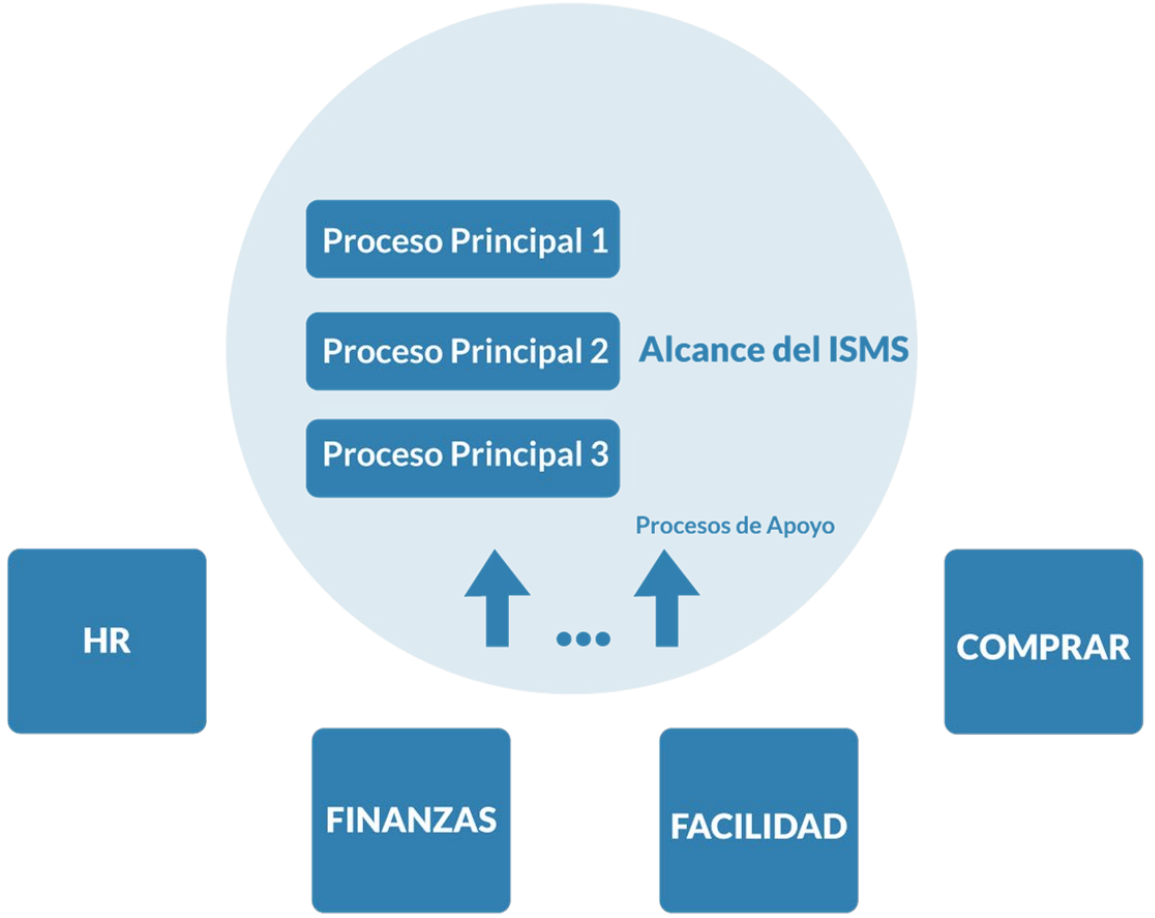


Fig 1: Mapa Gráfico del Alcance del SGSI

Estructura de ISO IEC 27001

Requisitos y cómo abordarlos

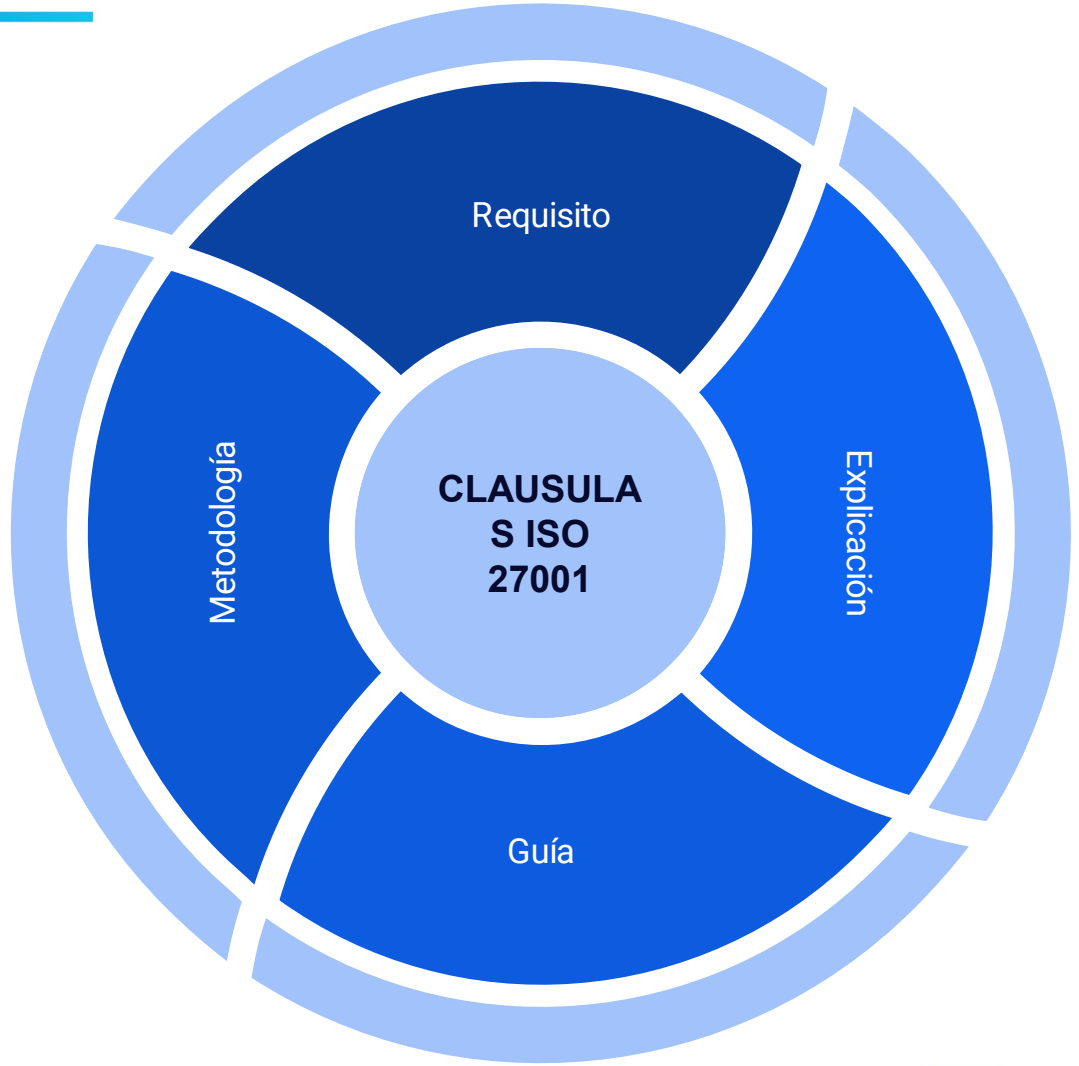
En este módulo se abordan los requisitos declarados en la cláusula 4 de la ISO IEC 27001:2022 desde 4 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 4 de la ISO 27001.

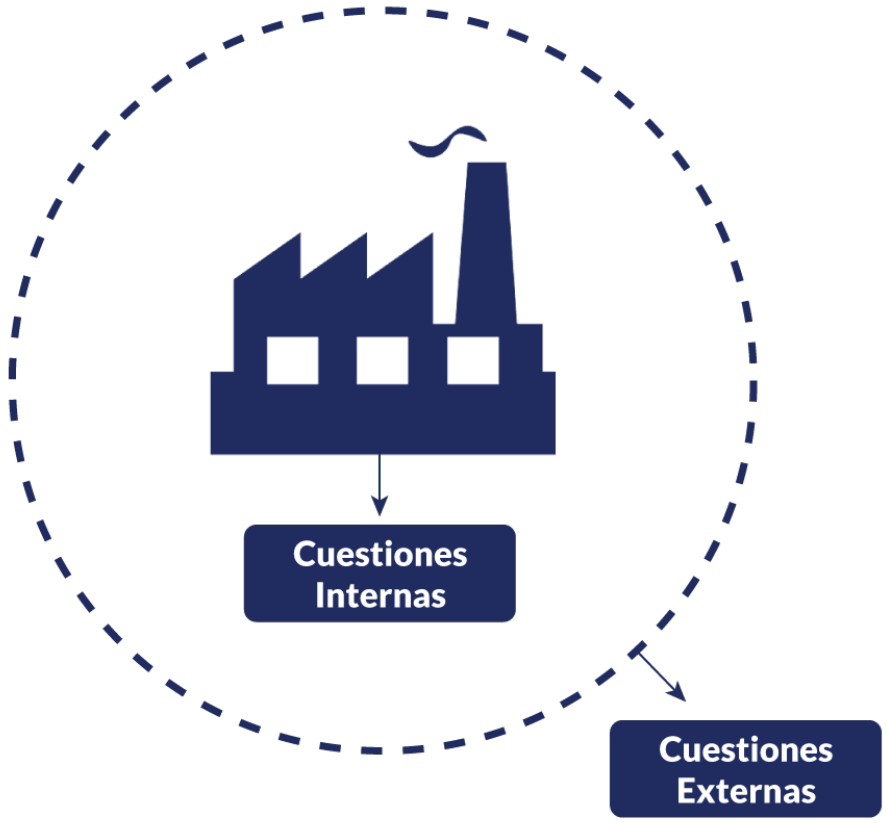
Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Metodología: Serie de métodos, técnicas, mejores prácticas y pasos recomendados para abordar los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarados en la cláusula 4 de la ISO 27001 (se incluye para el tema definido en el alcance del módulo).

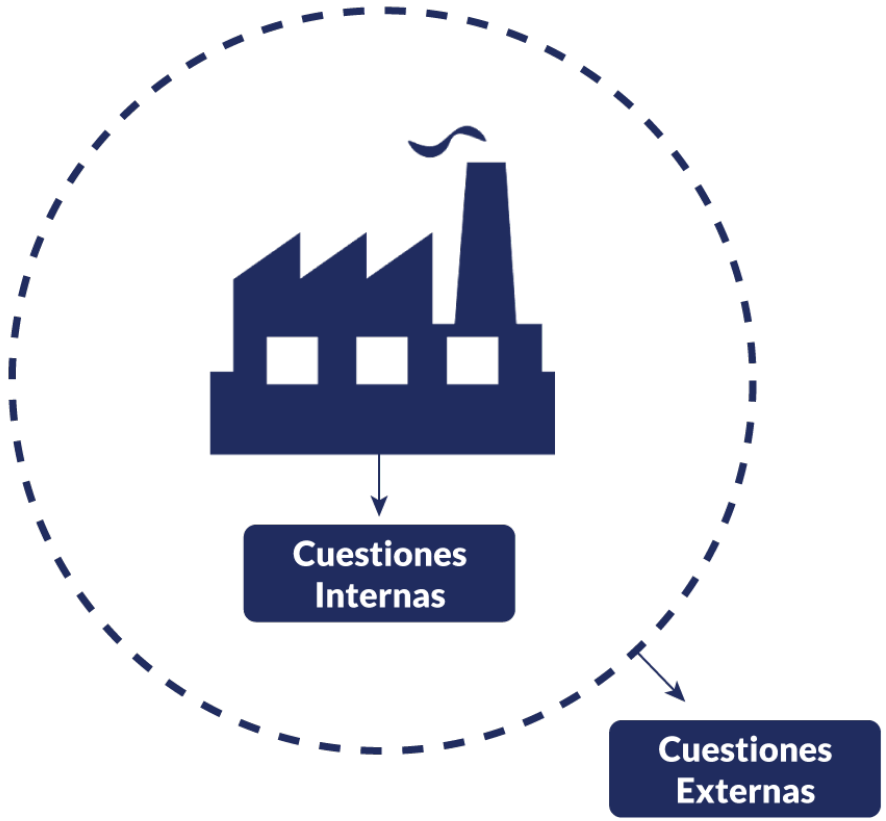


4.1 Comprensión de la Organización y su Contexto - Requisito



La organización determina cuestiones externas e internas relevantes para su propósito y que afectan su
capacidad para lograr los resultados previstos del sistema de gestión de seguridad de la información (SGSI).

4.1 Comprensión de la Organización y su Contexto - Explicación



Como una función integral del SGSI, la organización se **analiza** continuamente a sí misma y analiza el mundo que la rodea. Este análisis tiene que ver con **cuestiones externas e internas** que afectan de alguna manera la seguridad de la información y cómo se puede gestionar la seguridad de la información, y que son pertinentes a los objetivos de la organización.

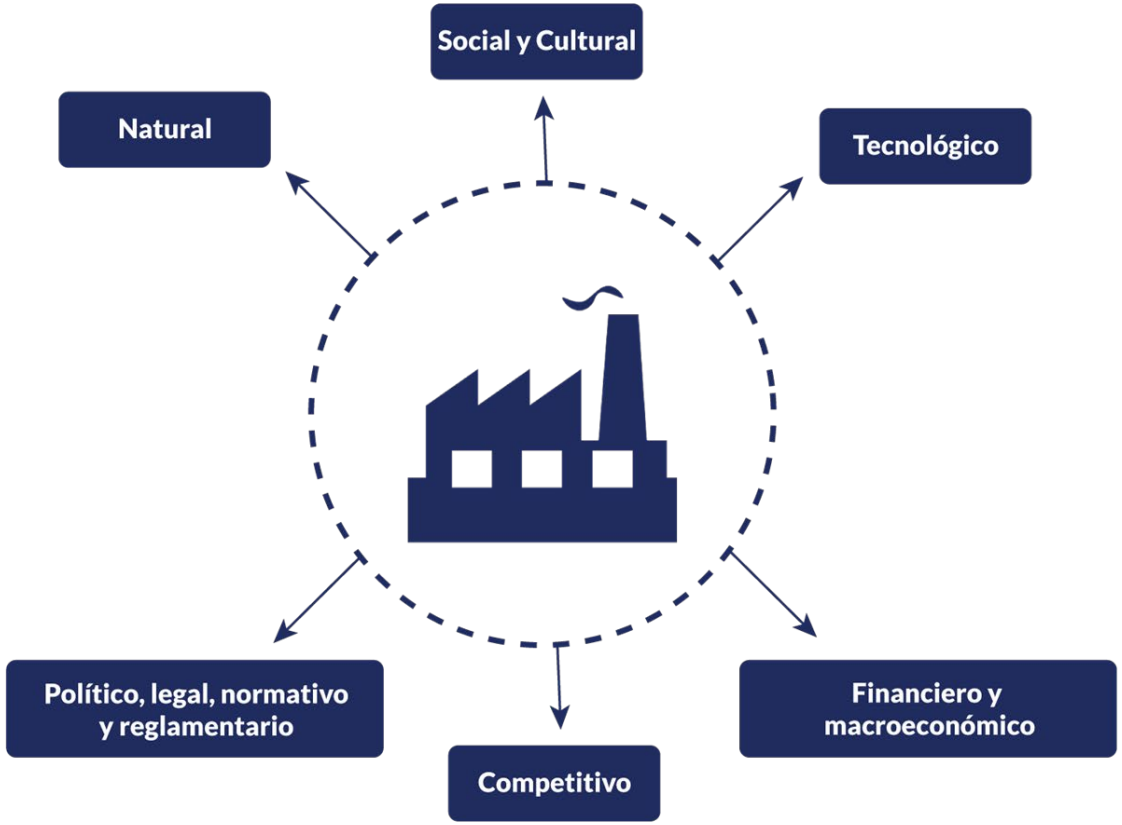
4.1 Comprensión de la Organización y su Contexto - Explicación

Los 3 propósitos del análisis cuestiones internas y externas

- Comprender el contexto para decidir el alcance del SGSI.
- Analizar el contexto para determinar los riesgos y las oportunidades.
- Asegurar que el SGSI está adaptado a las cuestiones externas e internas cambiantes.

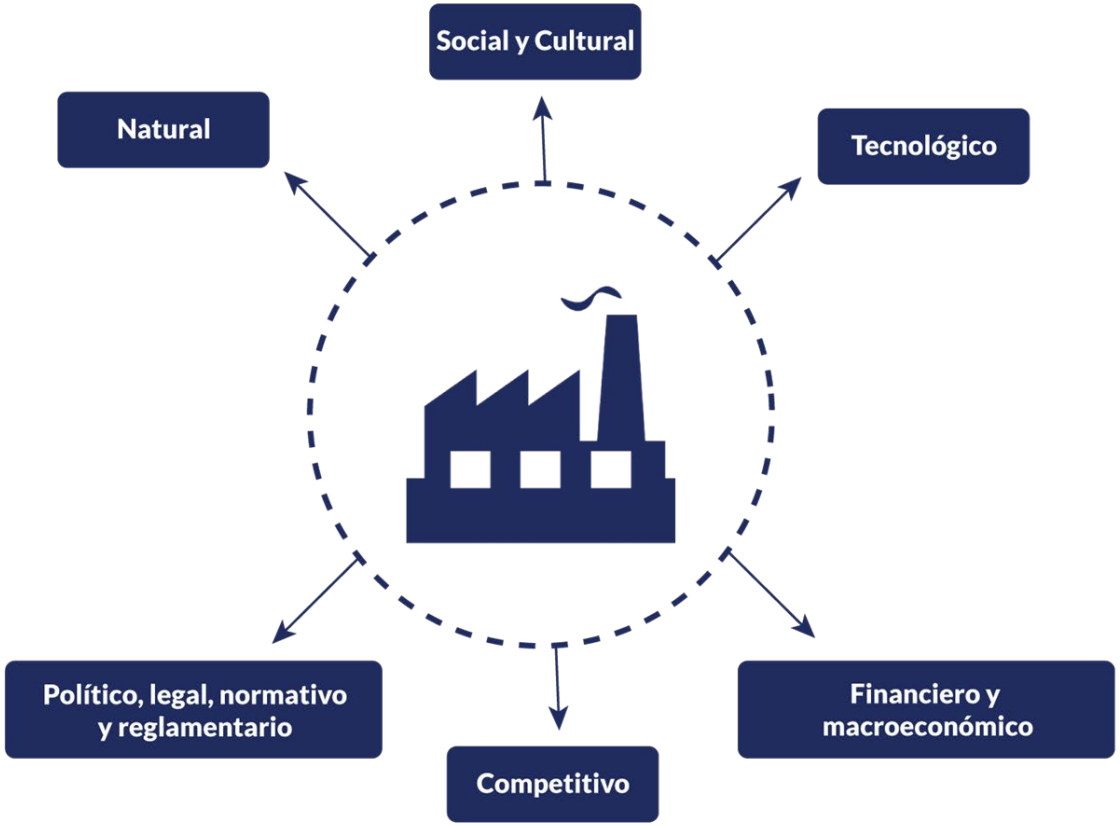
4.1 Comprensión de la Organización y su Contexto - Explicación

Las cuestiones externas son aquellos que están fuera del control de la organización. Esto a menudo se conoce como el entorno de la organización. El análisis de este entorno puede incluir los siguientes aspectos:



Estos aspectos del entorno de la organización presentan continuamente cuestiones que afectan la seguridad de la información y la manera en que ésta se puede gestionar.

4.1 Comprensión de la Organización y su Contexto - Explicación



Por ejemplo, los problemas externos para una organización específica pueden incluir:

Las implicaciones legales del uso de un servicio de TI subcontratado (aspecto legal);

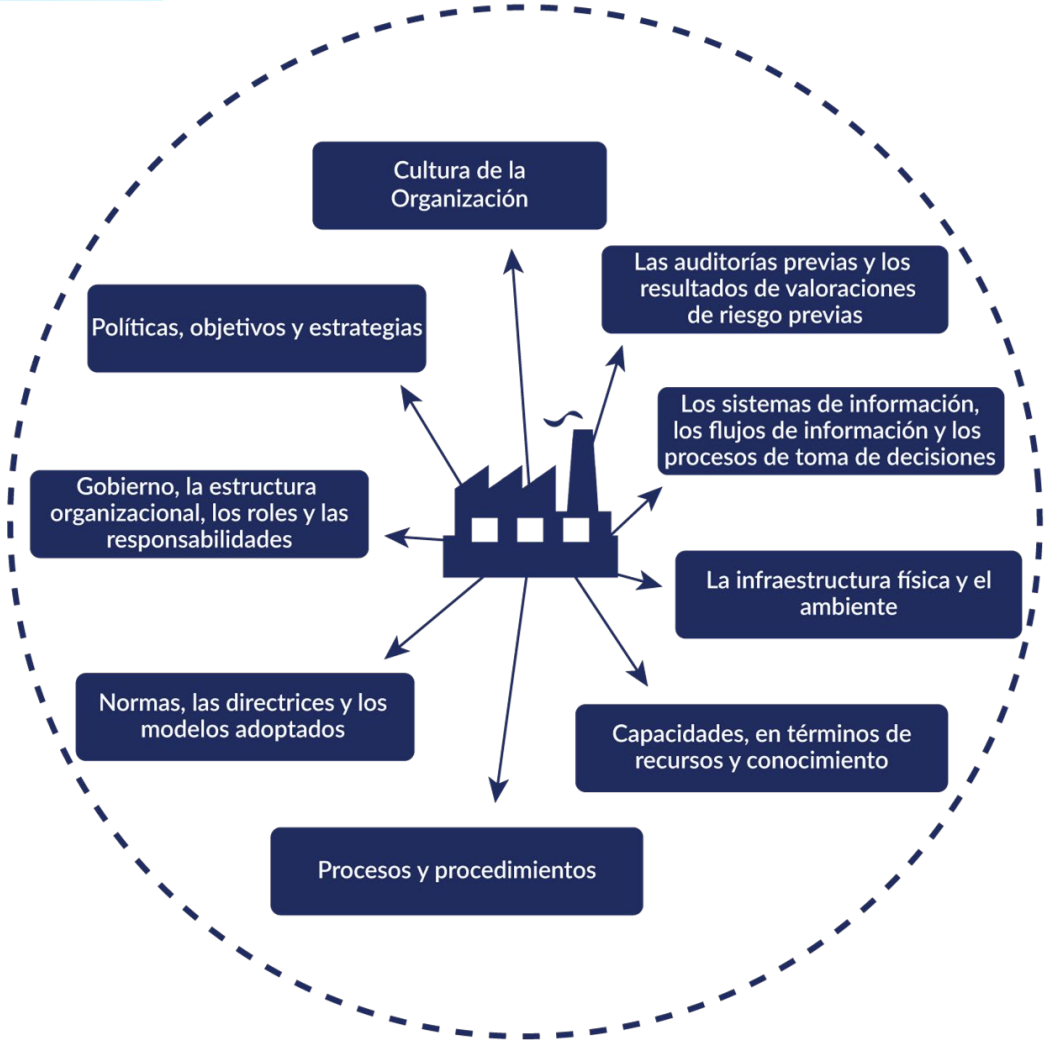
Características de la naturaleza en términos de posibilidad de desastres como incendios, inundaciones y terremotos (aspecto natural);

Avances técnicos de herramientas de hacking y uso de criptografía (aspecto tecnológico); y

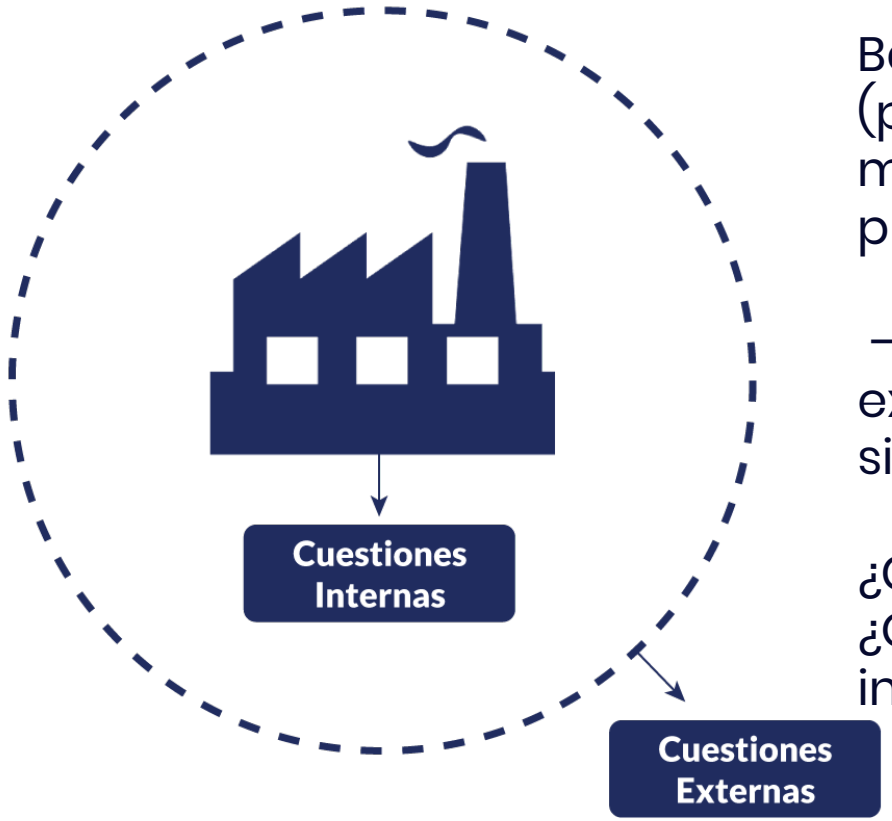
La demanda general de los servicios de la organización (aspectos sociales, culturales o financieros).

4.1 Comprensión de la Organización y su Contexto – Explicación

Las cuestiones internas están sujetos al control de la organización. El análisis de los problemas internos puede incluir los siguientes aspectos:



4.1 Comprensión de la Organización y su Contexto - Guía



Los resultados de esta actividad se pueden utilizar en las cláusulas : 4.3, 6.1 y 9.3.

Basado en la comprensión del propósito de la organización (por ejemplo, haciendo referencia a su declaración de misión o plan de negocios), así como los resultados previstos del SGSI de la organización, la organización debe:

— Revisar el entorno externo para identificar cuestiones externas e internas relevantes, se pueden plantear las siguientes preguntas:

¿Cómo funciona una determinada categoría?
¿Qué cuestiones afectan los objetivos de seguridad de la información?

4.1 Comprensión de la Organización y su Contexto - Guía

Ejemplo 1 Sobre gobernanza y estructura organizacional: Al establecer un SGSI, se deben tener en cuenta las estructuras organizativas y de gobernanza ya existentes.

Por ejemplo, la organización puede modelar la estructura de su SGSI basándose en la estructura de otros existentes sistemas de gestión y pueden combinar funciones comunes, como la revisión de la gestión y la auditoría.

Ejemplo 2 sobre políticas, objetivos y estrategias: Un análisis de las políticas, objetivos existentes y estrategias, pueden indicar lo que la organización pretende lograr y cómo se implementa la seguridad de la información.
Los objetivos se pueden alinear con los objetivos comerciales para garantizar resultados exitosos.

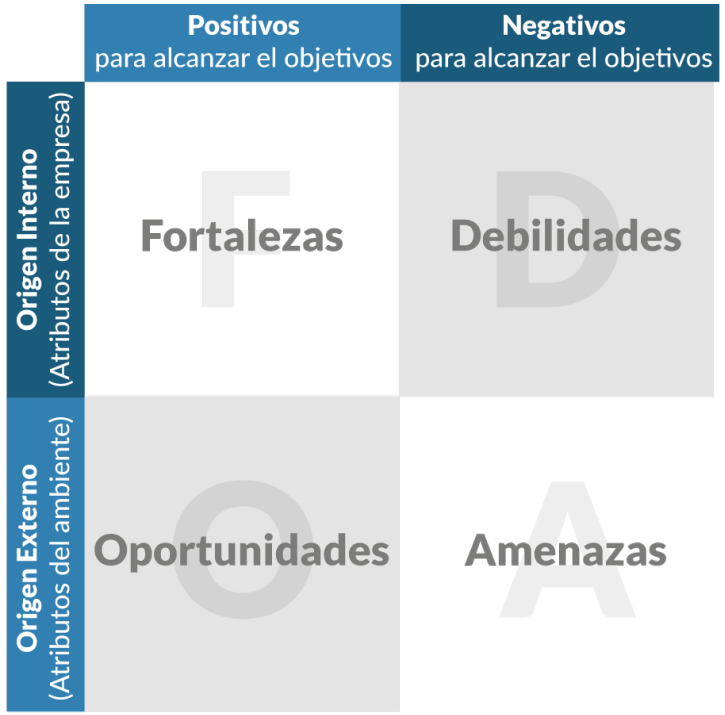
Ejemplo 3 sobre sistemas de información y flujos de información: Al determinar las cuestiones internas la organización debería identificar, con un nivel suficiente de detalle, los flujos de información entre sus diversos sistemas de información.

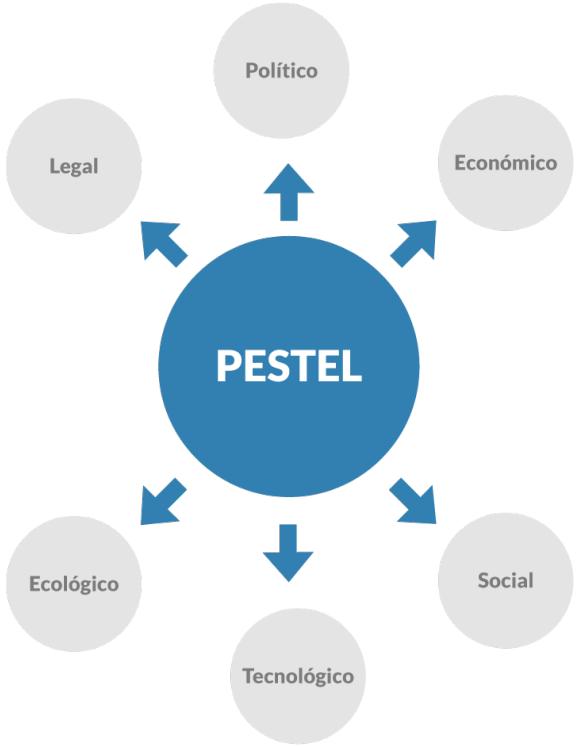
Tanto los problemas externos como los internos cambiarán con el tiempo, los problemas y su influencia en el alcance, las limitaciones y los requisitos del SGSI deben revisarse periódicamente.

La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y al medida que la organización considere necesaria para la eficacia de su sistema de gestión.

4.1 Comprensión de la Organización y su Contexto - Guía

- Herramientas para realizar el análisis interno y externo.
- FODA, PESTEL (PESTLE).





El método PESTLE puede ser usado para identificar los problemas externos que afectan a un sistema de gestión de seguridad de la información.

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas – Requisito

La organización determina las **partes interesadas** relevantes para el SGSI y sus requisitos relevantes para seguridad de información.

Partes Interesadas Internas

Partes Interesadas Externas

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas – Explicación

La organización determina las **partes interesadas** relevantes para el SGSI y sus requisitos relevantes para seguridad de información.

Parte interesada es un término que hace referencia a personas u organizaciones que pueden afectar o verse afectadas o percibirse afectadas por una decisión o actividad de la organización.

Las partes interesadas se pueden encontrar tanto dentro como fuera de la organización y pueden tener necesidades, expectativas y requisitos específicos para la seguridad de la información de la organización.

Partes Interesadas Internas

Partes Interesadas Externas

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas – Explicación

Partes Interesadas Internas

- Las personas encargadas de la toma de decisiones, incluida la alta dirección
- Los dueños de los procesos, los dueños de los sistemas y los dueños de la información
- Funciones de soporte tales como TI o recursos humanos
- Empleados y usuarios
- Profesionales en seguridad de la información

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas – Explicación

Partes Interesadas Externas

- Reguladores y legisladores
- Accionistas, incluidos los propietarios y los inversionistas
- Proveedores, incluidos los subcontratistas, consultores y socios por contratación externa
- Asociaciones industriales
- Competidores
- Clientes y consumidores
- Grupos de activistas

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas – Guía

- Se deben tomar los siguientes pasos:
  - Identificar partes interesadas externas;
  - Identificar las partes interesadas internas; y
  - Identificar las necesidades de las partes interesadas.

- A medida que las necesidades, expectativas y Requisitos de las partes interesadas cambian con el tiempo, estos cambios y su influencia en el alcance, las limitaciones y los requisitos del SGSI debe revisarse periódicamente.

- La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y medida que la organización considere necesaria para la eficacia de su sistema de gestión.

4.3 Determinación del Alcance del SGSI - Requisito

La organización determina los límites y la aplicabilidad del SGSI para establecer su alcance.

4.3 Determinación del Alcance del SGSI - Explicación

La organización determina los límites y la aplicabilidad del SGSI para establecer su alcance.

- El alcance define en dónde y para qué es aplicable exactamente el SGSI y en dónde y para qué no lo es.

- Establecer el alcance es una actividad clave que determina el fundamento necesario para todas las otras actividades en la implementación del SGSI

4.3 Determinación del Alcance del SGSI - Explicación

Definir, dónde exactamente es aplicable el SGSI, el conocimiento preciso de los límites y aplicabilidad del SGSI, las interfaces y dependencias entre la organización y otras organizaciones es fundamental, ya que cualquier modificación posterior del alcance puede generar considerables esfuerzos y costos adicionales.

Los siguientes factores pueden afectar la determinación del alcance:

a) Las cuestiones externas e internas descritas en 4.1;
b) Los interesados y sus requisitos que se determinan conforme a 4.2;
c) La preparación de las actividades comerciales para ser incluidas como parte de la cobertura del SGSI;
d) Todas las funciones de apoyo, es decir, funciones necesarias para respaldar estas actividades comerciales,
- -Recursos humanos;
- Servicios de TI;
- Aplicaciones de software;
- Instalaciones de edificios, zonas físicas:
- Servicios críticos que pueden causar un gran impacto en la organización o en sus clientes y partes interesadas como resultado de pérdidas de confidencialidad, integridad o disponibilidad y sus dependencias;
- Límites de la Tecnología de Comunicación de Información (TIC); y

e) Todas las funciones que se subcontratan a otras partes dentro de la organización o a empresas independientes. proveedores.

4.3 Determinación del Alcance del SGSI - Explicación

El alcance de un SGSI puede ser muy diferente de una implementación a otra. Por ejemplo, el alcance puede incluir:

— Uno o más procesos específicos;
— Una o más funciones específicas;
— Uno o más servicios específicos;
— Una o más secciones o ubicaciones específicas;
— Toda una entidad jurídica; y
— Toda una entidad administrativa y uno o más de sus proveedores.

4.3 Determinación del Alcance del SGSI - Guía

Para establecer el **alcance de un SGSI** se puede seguir un enfoque multietapas:

DETERMINAR EL ALCANCE PRELIMINAR

Esta actividad la debería llevar a cabo un grupo pequeño pero representativo de representes de la dirección.

DETERMINAR EL ALCANCE PERFECCIONADO

Las unidades funcionales dentro y fuera del alcance preliminar se deberían revisar, y posiblemente luego se deberían incluir o excluir algunas de estas unidades funcionales para reducir el número de interfaces a lo largo de los límites.

DETERMINAR EL ALCANCE FINAL

El alcance perfeccionado debería ser evaluado por toda la dirección dentro del alcance perfeccionado. Si es necesario, se debería ajustar y luego describir con precisión.

LA APROBACIÓN DEL ALCANCE

La información documentada que describe el alcance la debería aprobar formalmente la alta dirección.

4.3 Determinación del Alcance del SGSI - Guía

La organización también debe considerar actividades con impacto en el SGSI o actividades que sean subcontratadas, ya sea a otras partes dentro de la organización o a proveedores independientes.

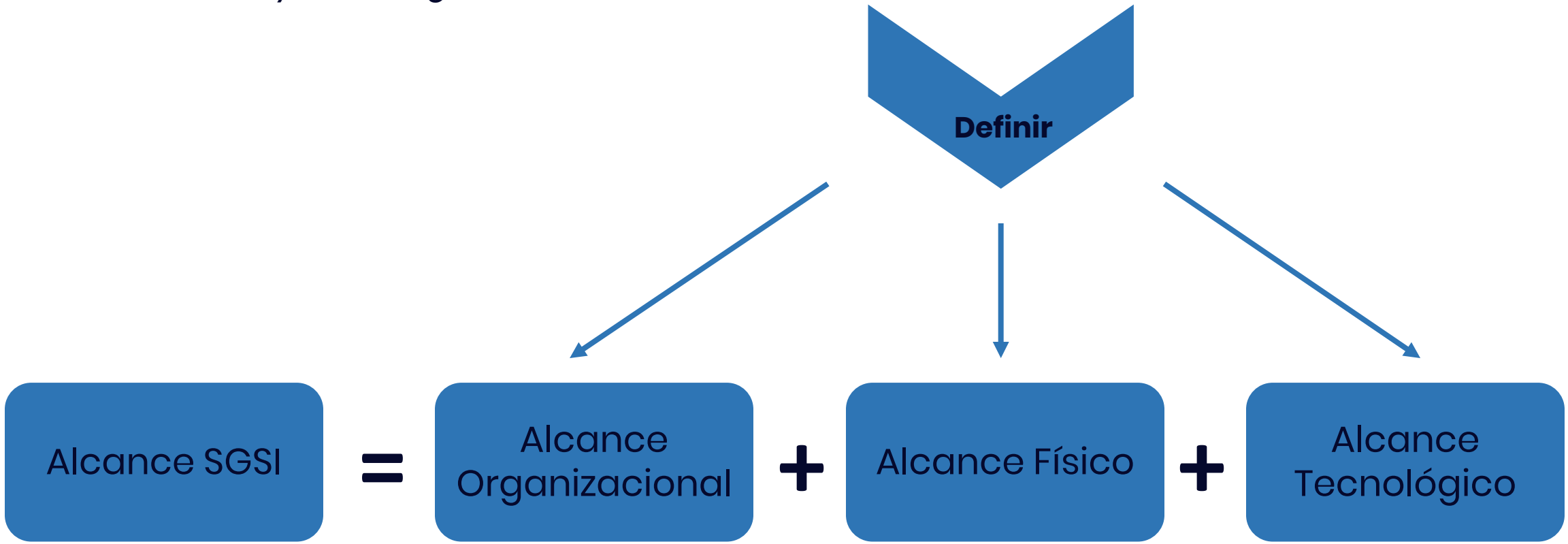
Para tales actividades, interfaces (físicas, técnicas y organizativas) y su influencia en el alcance deben ser identificadas.

La información documentada que describe el alcance debe incluir:

- El alcance, los límites y las interfaces de la organización;
- El alcance, los límites y las interfaces de las tecnologías de la información y las comunicaciones; y
- El alcance físico, límites e interfaces.

4.3 Determinación del Alcance del SGSI - Metodología

"Definir el alcance del SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología".



4.3 Determinación del Alcance del SGSI - Metodología

Pasos:

1 Alcance Organizacional

A partir de la descripción de los procesos y la estructura de la organización.

2 Alcance Físico

Considerando las diferentes sedes y la distribución física de las diferentes áreas de la organización.

3 Alcance Tecnológico

A partir de los diagramas y descripciones de la infraestructura tecnológica.

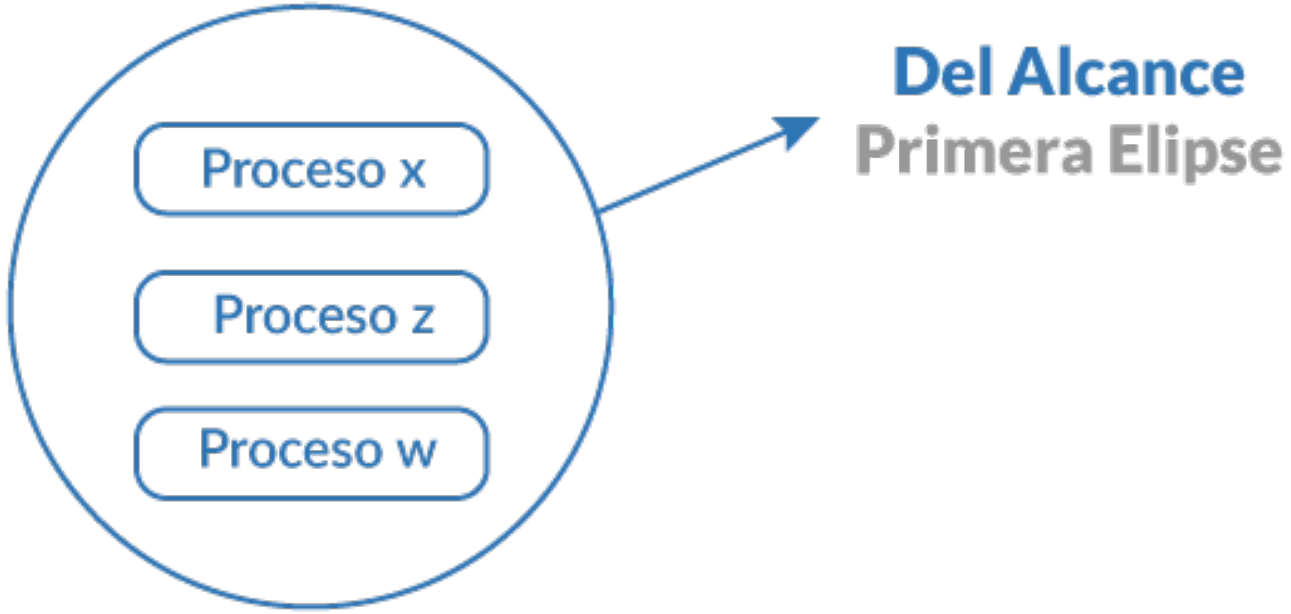
4 Integración

Las 3 dimensiones y plantear una justificación para las eventuales exclusiones al alcance del SGSI.

4.3 Determinación del Alcance del SGSI - Metodología

Método de Elipses

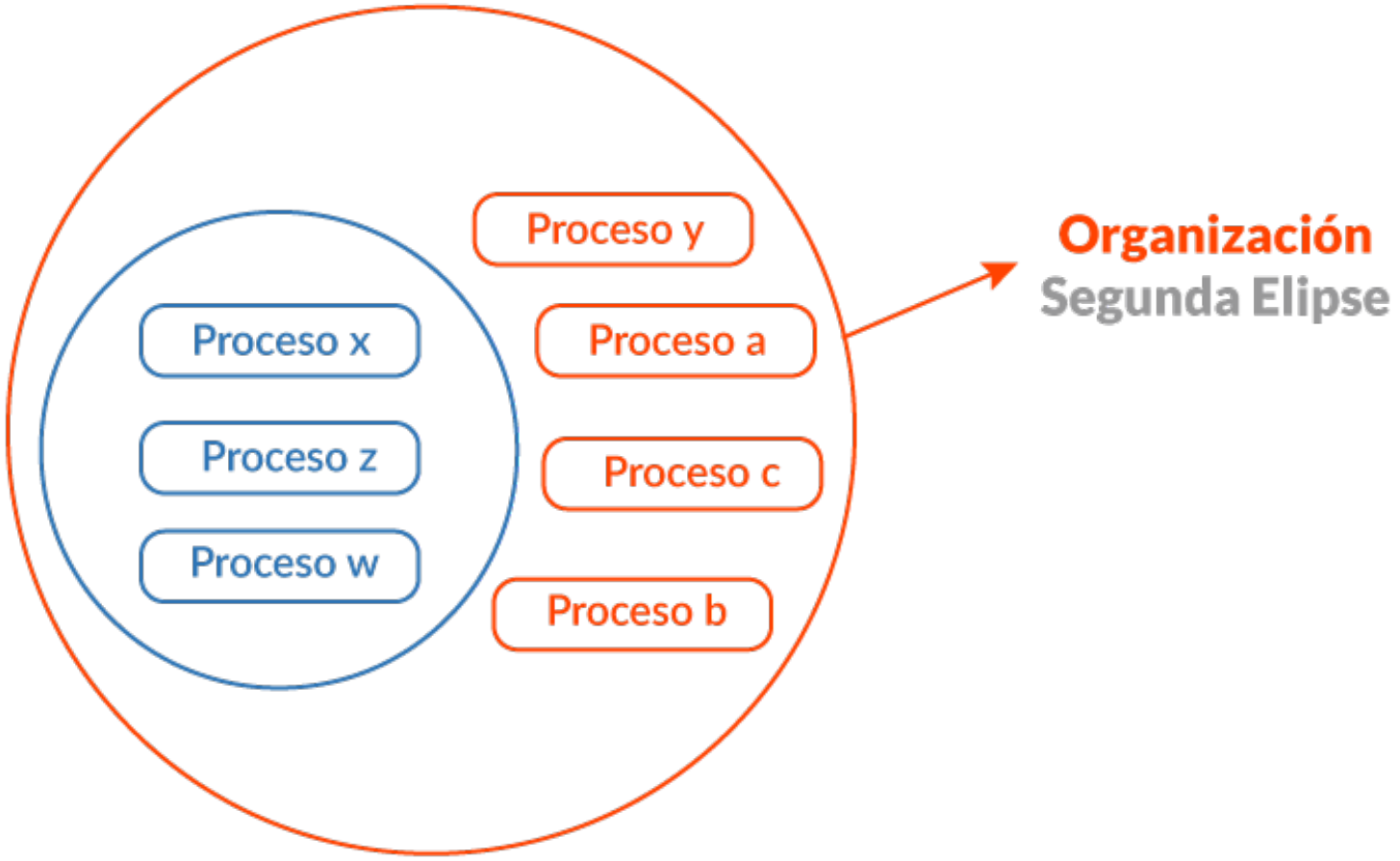
1. Ubique los procesos de mayor relevancia dentro de la elipse del alcance.



4.3 Determinación del Alcance del SGSI - Metodología

Método de Elipses

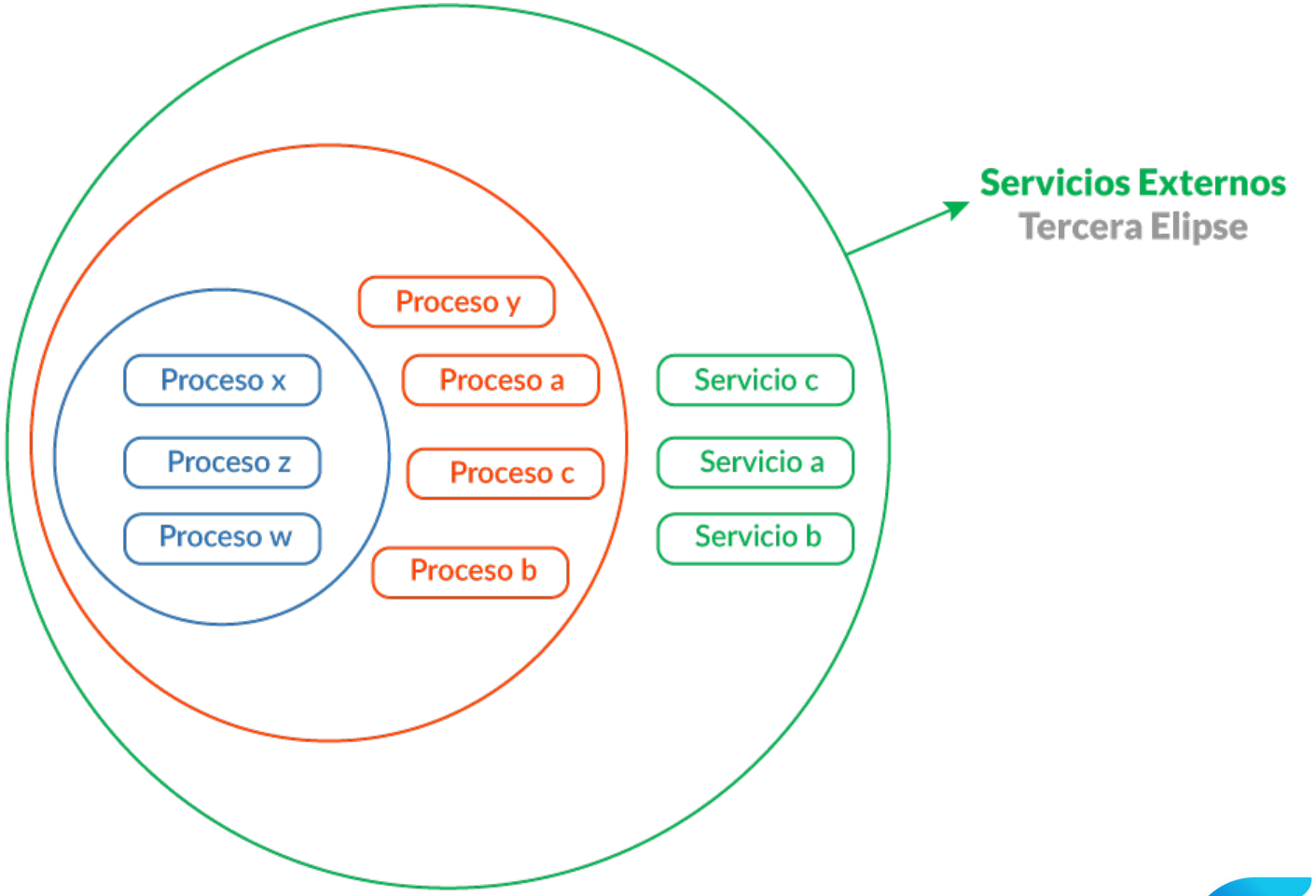
2 Ubique los demás procesos de acuerdo a las características propias de la organización.



4.3 Determinación del Alcance del SGSI - Metodología

Método de Elipses

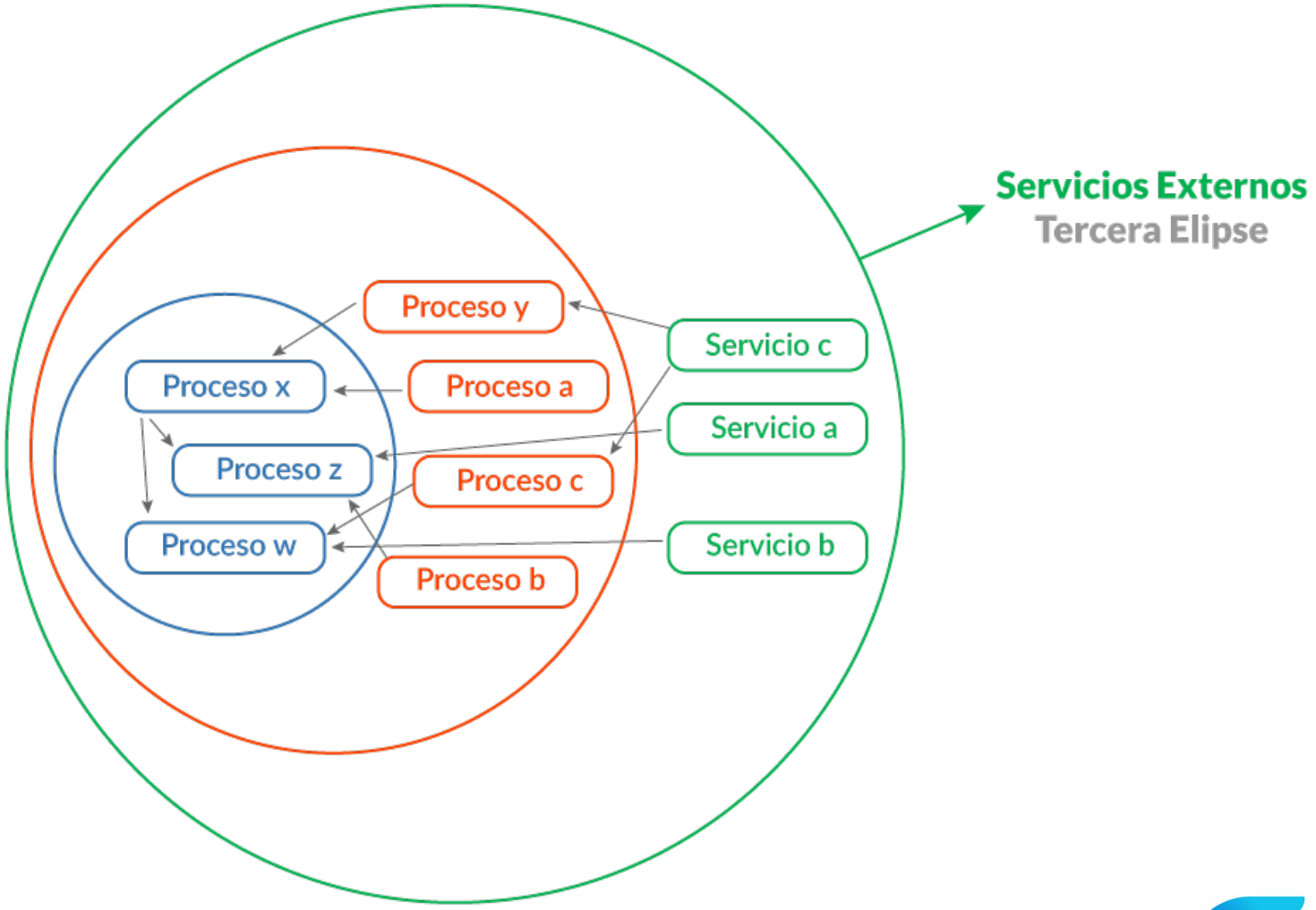
3 Ubique aquellos servicios externos que tienen interacción con los procesos del alcance.



4.3 Determinación del Alcance del SGSI - Metodología

Método de Elipses

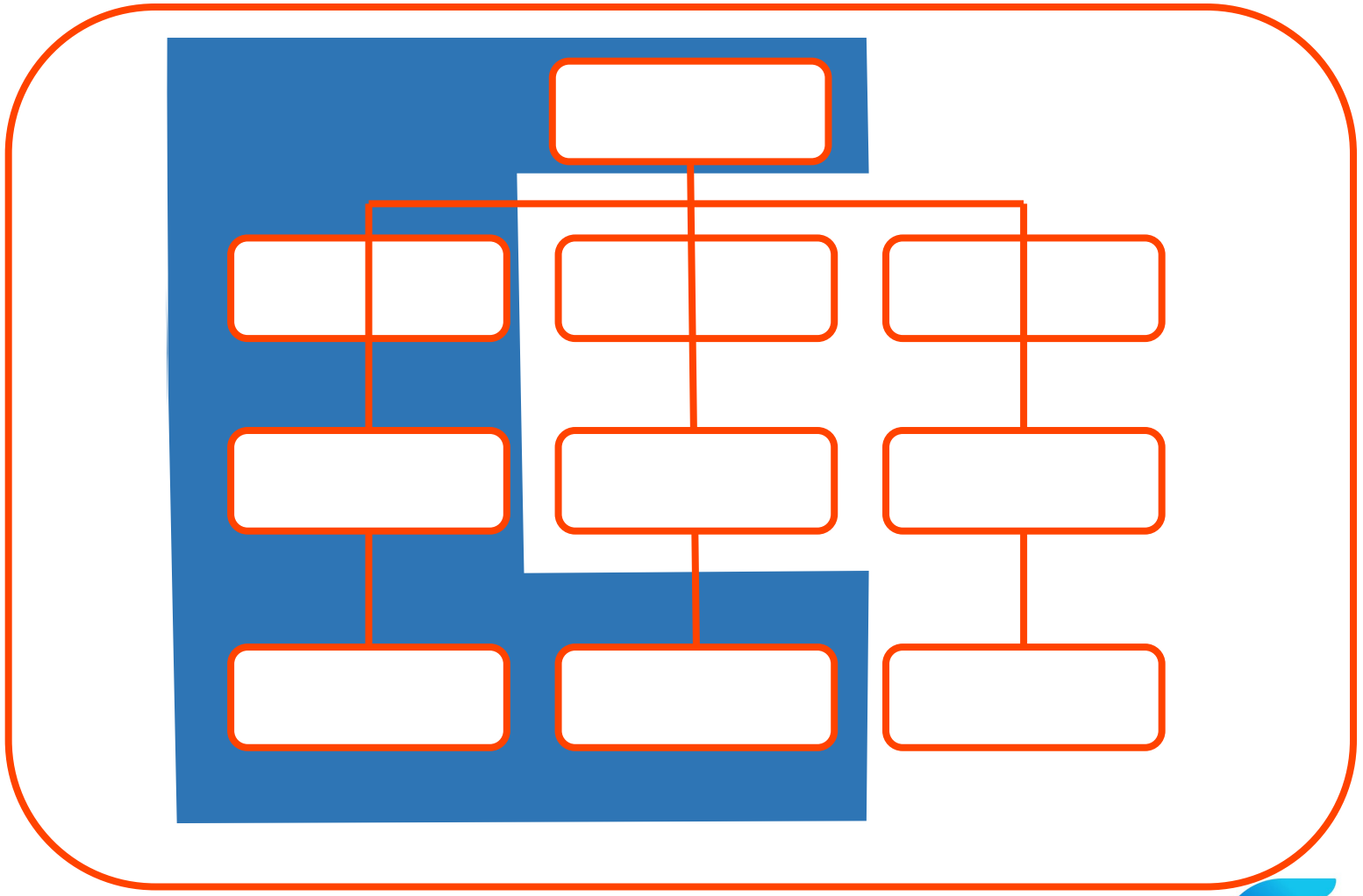
4 Trace las interrelaciones entre los procesos de acuerdo con la descripción de las interacciones e interrelaciones entre los mismos.



4.3 Determinación del Alcance del SGSI - Metodología

Diagrama estructural funcional

- Plantee un diagrama de la estructura funcional de la organización.
- Identifique las áreas incluidas en el alcance planteado.
- Resalte las líneas de mando y demás información relevante para la seguridad.



4.3 Determinación del Alcance del SGSI - Metodología

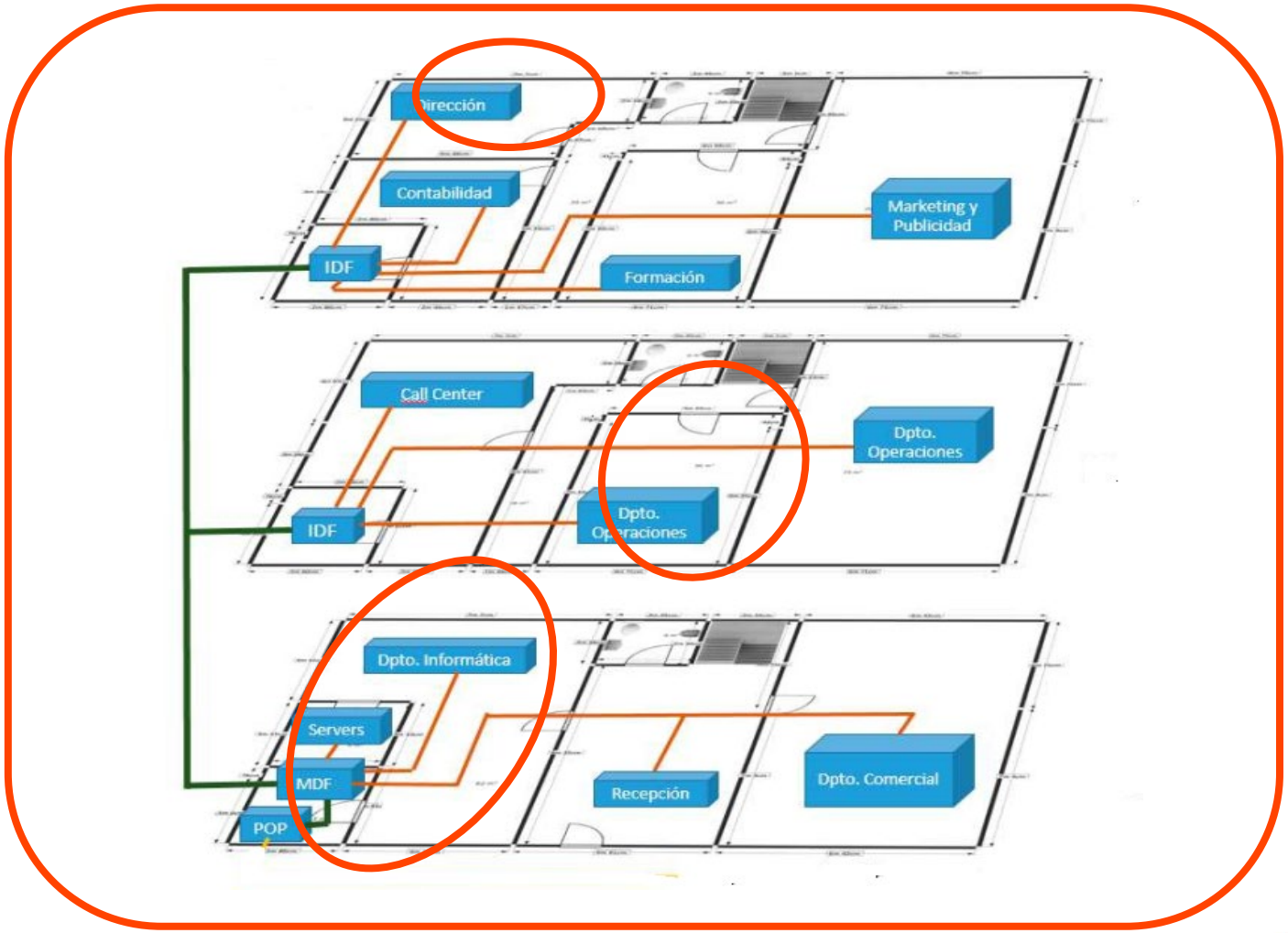
Diagrama planta física

- Represente, en un diagrama, la planta física de la organización.
- Identifique las áreas incluidas en el alcance planteado.
- Resalte los puntos de acceso, barreras físicas, facilidades y demás información relevante para la seguridad.

4.3 Determinación del Alcance del SGSI - Metodología

Diagrama planta lógica

- Represente en un diagrama la organización lógica de la red y los servicios de TI de la organización.
- Identifique las áreas incluidas en el alcance planteado.
- Resalte las puertas de enlace, enrutadores, barreras de fuego, equipos activos, servicios, actores, facilidades y demás información relevante para la seguridad.



4.4 Sistema de gestión de seguridad de la información – Requisito

La organización establece, implementa, mantiene y mejora continuamente el SGSI.

SGSI

4.4 Sistema de gestión de seguridad de la información – Explicación

La norma ISO IEC 27001:2022, en su cláusula 4.4 establece el requisito central para establecer, implementar y mantener y mejorar continuamente un SGSI.

Mientras que las otras cláusulas de la ISO IEC 27001 describen los requisitos de un SGSI, la cláusula 4.4 exige a la organización garantizar que todos los elementos requeridos se cumplan para establecer, implementar, mantener y mejorar continuamente el SGSI.

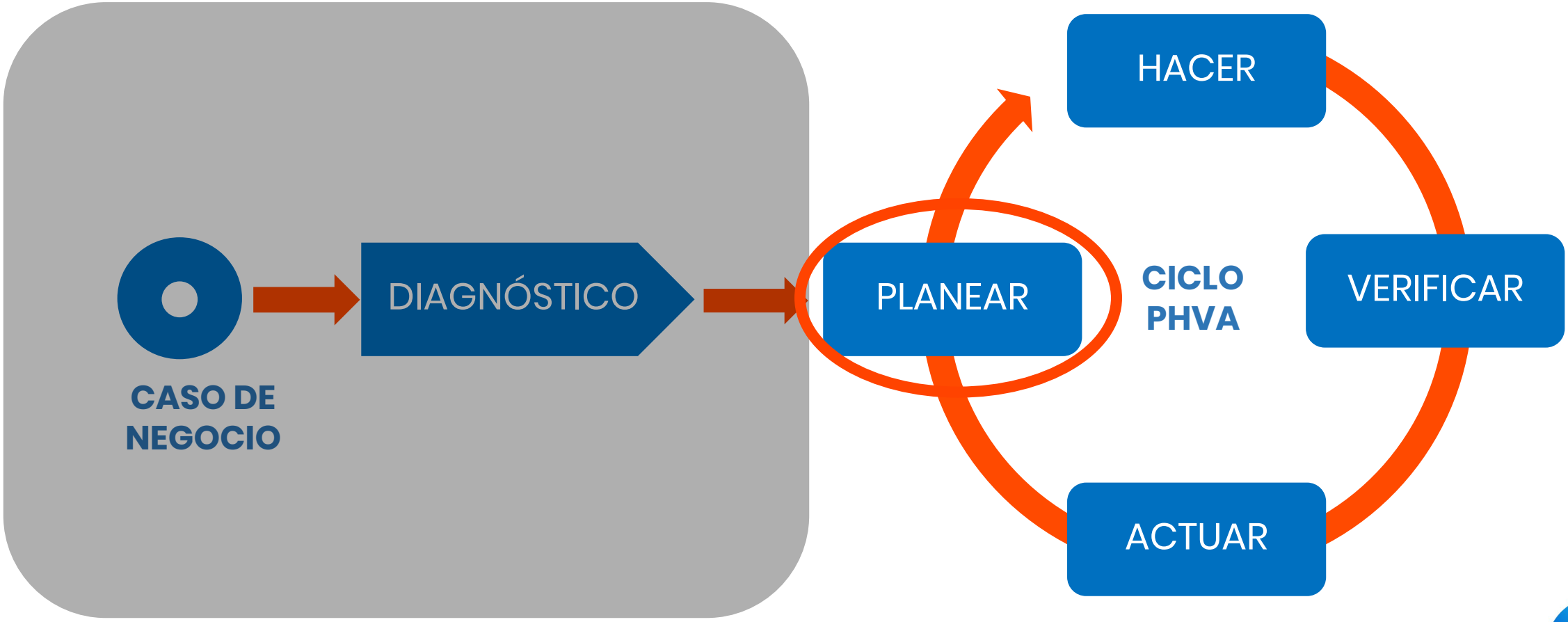
SGSI

5. Liderazgo: Interpretar los Requisitos ISO IEC 27001

5.1 Liderazgo y Compromiso.
5.2 Políticas.
5.3 Roles, Responsabilidades y Autoridades Organizacionales.

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (Planear) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de diseñar una política del ISMS.

Estructura de ISO IEC 27001

Requisitos y cómo abordarlos

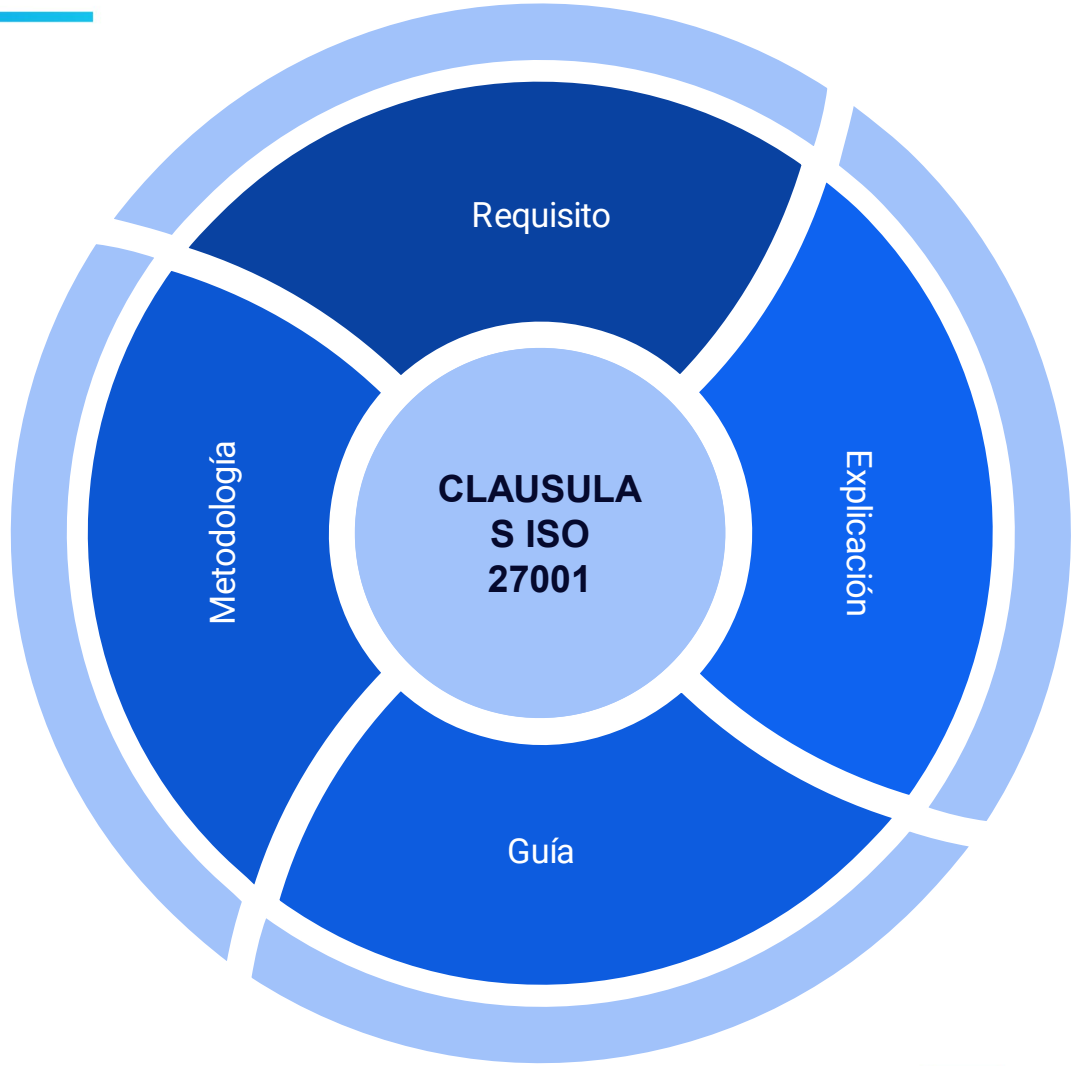
En este módulo se abordan los requisitos declarados en la cláusula 5 de la ISO IEC 27001:2022 desde 4 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 5 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Metodología: Serie de métodos, técnicas, mejores prácticas y pasos recomendados para abordar los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarados en la cláusula 5 de la ISO 27001 (se incluye para el tema definido en el alcance del módulo).



5.1 Liderazgo y Compromiso - Requisito

La alta dirección demuestra liderazgo y compromiso con respecto al SGSI.

5.1 Liderazgo y Compromiso - Explicación

El liderazgo y el compromiso son esenciales para un SGSI eficaz.

- La **Alta Dirección se define como** una persona o grupo de personas que dirige y controla la organización del SGSI al nivel más alto, es decir, la alta dirección tiene la responsabilidad total por el SGSI; la organización que implementa y opera el SGSI puede ser una unidad de negocios dentro de una organización más grande, en este caso, la alta dirección es la persona o grupo de personas que dirige y controla esa unidad de negocio.

5.1 Liderazgo y Compromiso - Explicación

- La **Alta Dirección** puede delegar autoridad en la organización y proporcionar recursos para ejecutar realmente las actividades relacionadas con seguridad de la información y el SGSI **pero aún conserva la responsabilidad general.**

- La **Alta Dirección** también participa en la revisión del SGSI (responsabilidad declarada en la cláusula 9 de la ISO IEC 27001:2022) y promueve la mejora continua responsabilidad declarada en la cláusula 10 de la ISO IEC 27001:2022.

5.1 Liderazgo y Compromiso - Guía

La Alta Dirección debe demostrar liderazgo y mostrar compromiso al:

- **Asegurar** que se establezcan la política de seguridad de la información y los objetivos de seguridad de la información y que sean compatibles con la dirección estratégica de la organización.
- **Asegurar** que los requisitos y controles del SGSI estén integrados a los procesos de la organización.

Por ejemplo, una organización que ha designado propietarios de procesos puede delegar la responsabilidad de implementar los requisitos aplicables a estas personas o grupo de personas, sin embargo, la responsabilidad final recae sobre la alta dirección.
El apoyo de la dirección también puede ser necesario para superar la resistencia organizacional a los cambios en procesos y controles implementados.

5.1 Liderazgo y Compromiso - Guía

- **Asegurar** la disponibilidad de recursos para un SGSI eficaz son necesarios para el establecimiento, mantenimiento y mejora, así como para la implementación de los controles.

  Los recursos necesarios para el SGSI incluyen:
  1. Recursos financieros.
  2. Personal.
  3. Instalaciones.
  4. Infraestructura técnica.

  Los recursos necesarios dependen del contexto de la organización, como el tamaño, la complejidad y requisitos internos y externos. La revisión por la dirección debe proporcionar información que indica si los recursos son adecuados para la organización.

- **Comunicar** la necesidad de gestión de la seguridad de la información en la organización y la necesidad de cumplir los requisitos del SGSI, esto se puede hacer dando ejemplos prácticos que ilustran cuál es la necesidad real en el contexto de la organización y comunicar los requisitos de seguridad de la información.

5.1 Liderazgo y Compromiso - Guía

- **Asegurar** que el SGSI logre el(los) resultados previstos apoyando la implementación de todos los procesos de gestión de la seguridad de la información, y en particular solicitando y revisando informes sobre el estado y la eficacia del SGSI, Tales informes pueden derivarse de mediciones, revisiones de la dirección e informes de auditoría (cláusula 9), La alta dirección también puede establecer objetivos de desempeño para el personal clave involucrado con el SGSI.

- **Dirigir** y **Apoyar** a las personas de la organización que están involucradas directamente con la seguridad de la información y el SGSI, la retroalimentación de la alta dirección puede incluir cómo se alinean las actividades planificadas con las necesidades estratégicas para la organización y también para priorizar diferentes actividades en el SGSI.

- **Hacer** una valoración de las necesidades de recursos durante las revisiones por la dirección y establecer los objetivos para la mejora continua y para hacer seguimiento a la eficacia de las actividades planificadas.

5.1 Liderazgo y Compromiso - Guía

- **Apoyar** a las personas a las cuales se les han asignado roles y responsabilidades relacionadas con la gestión de la seguridad de la información, de manera que estén motivadas y estén en capacidad de dirigir y apoyar actividades de seguridad de la información dentro de su área.

En los casos en que la organización que implementa y opera un SGSI es parte de una organización más grande el liderazgo y el compromiso pueden mejorarse mediante el compromiso con la persona o grupo de personas que controla y dirige la organización más grande. Si entienden lo que implica implementar un SGSI, pueden proporcionar apoyo a la alta dirección dentro del alcance del SGSI y ayudarles a proporcionar liderazgo y demostrar compromiso con el SGSI.

Por ejemplo, si partes interesadas fuera del alcance del SGSI participan en la toma de decisiones relativas a los objetivos, riesgos y criterios de seguridad de la información, y se mantienen al tanto de los resultados producidos por el SGSI, sus decisiones con respecto a la asignación de recursos se pueden alinear con los requisitos del SGSI.

5.2 Política – Requisito

La alta dirección establece una política de seguridad de la información.

5.2 Políticas – Explicación

La alta dirección establece una política de seguridad de la información.

La política de seguridad de la información describe la importancia estratégica del SGSI para la organización y está disponible como información documentada.

La política de seguridad de la información dirige las actividades de seguridad de la información en la organización.

La política de seguridad de la información establece cuáles son las necesidades de seguridad de la información en el contexto real de la organización.

El propósito más importante de **la política de seguridad de la información es** proporcionar a la organización dirección y apoyo a la gestión en materia de seguridad de la información.

5.2 Políticas – Guía

- **La política de seguridad de la información** debe contener declaraciones de intención y dirección breves y de alto nivel y referentes a la seguridad de la información. Puede ser específico del alcance de un SGSI o puede tener una cobertura más amplia. Todas las demás políticas, procedimientos, actividades y objetivos relacionados con la seguridad de la información deben ser alineados a la política de seguridad de la información.
- **La política de seguridad de la información** debe reflejar la situación empresarial, la cultura, los problemas y las preocupaciones relacionadas con la seguridad de la información.
- El alcance de **la política de seguridad de la información** debe estar de acuerdo con el propósito y la cultura de la organización y debe buscar un equilibrio entre facilidad de lectura y exhaustividad. Es importante que los usuarios de la póliza puedan identificarse con la dirección estratégica de la política.

5.2 Políticas – Guía

- **La política de seguridad de la información** puede incluir objetivos de seguridad de la información para la organización o describir el marco sobre cómo se establecen los objetivos de seguridad de la información (es decir, quién los establece para el SGSI y cómo deben implementarse dentro del alcance del SGSI). Por ejemplo, en muy grandes organizaciones, los objetivos de alto nivel deben ser establecidos por la alta dirección de toda la organización, luego, de acuerdo a un marco establecido en la política de seguridad de la información, los objetivos deben ser detallado de manera que dé un sentido de dirección a todas las partes interesadas.
- **La política de seguridad de la información** debe contener una declaración clara de la alta dirección sobre su compromiso de satisfacer los requisitos relacionados con la seguridad de la información.
- **La política de seguridad de la información** debe contener una declaración clara de que la alta dirección apoya la mejora continua en todas las actividades. Es importante establecer este principio en la política, de modo que las personas dentro del alcance del SGSI sean conscientes de ello.

5.2 Políticas – Guía

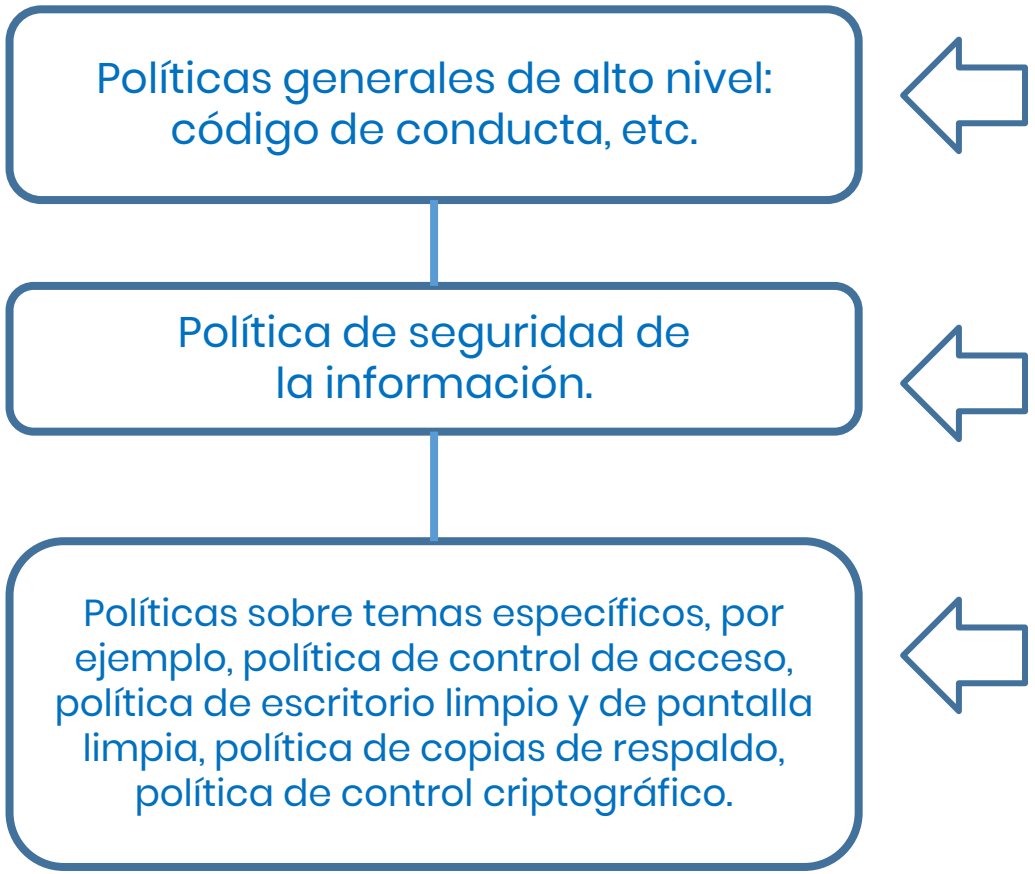
- **La política de seguridad de la información** debe comunicarse a todas las personas dentro del alcance del SGSI. Por lo tanto, su formato y lenguaje deben ser adecuados para que sea fácilmente comprensible para todos.
  La alta dirección debe decidir a qué partes interesadas se debe comunicar la política.
  La política de seguridad de la información se puede redactar de tal manera que sea posible comunicar a las autoridades pertinentes y partes interesadas externas ajenas a la organización. Si la política de seguridad de la información se pone a disposición de partes interesadas externas, no debe incluir información confidencial.
- **La política de seguridad de la información** puede ser una política independiente o estar incluida en una política integral, que cubre múltiples temas del sistema de gestión dentro de la organización.
- **La política de seguridad de la información** debe estar disponible como información documentada. Los requisitos en la ISO IEC 27001:2022 no implica ningún formato específico como información documentada, y por lo tanto depende de la organización decidir qué formato es el más apropiado. Si la organización tiene una plantilla estándar para las políticas, puede utilizar esta plantilla.

5.2 Políticas – Guía

- **La política de seguridad de la información** es una declaración de intenciones y dirección de una organización tal como se expresa formalmente por su alta dirección.
- El contenido de una política orienta las acciones y decisiones relativas al tema de la política.
- Una organización puede tener varias políticas; uno para cada una de las áreas de actividad que es importante para la organización.
- Algunas políticas son independientes entre sí, mientras que otras tienen una relación jerárquica.

5.2 Políticas – Guía

JERARQUÍA DE POLÍTICAS



La política general se apoya en otras políticas que abordan diferentes temas y puede ser aplicable a áreas o funciones específicas de la organización.

La política de seguridad de la información es una de estas políticas, la política de seguridad de la información está respaldada por una variedad de políticas temáticas específicas relacionadas con aspectos de seguridad de información. Varios de ellos se analizan en ISO IEC 27002:2022, Tenga en cuenta que algunas organizaciones utilizan otros términos para documentos de políticas sobre temas específicos, como “estándares”, “directivas” o “reglas”.

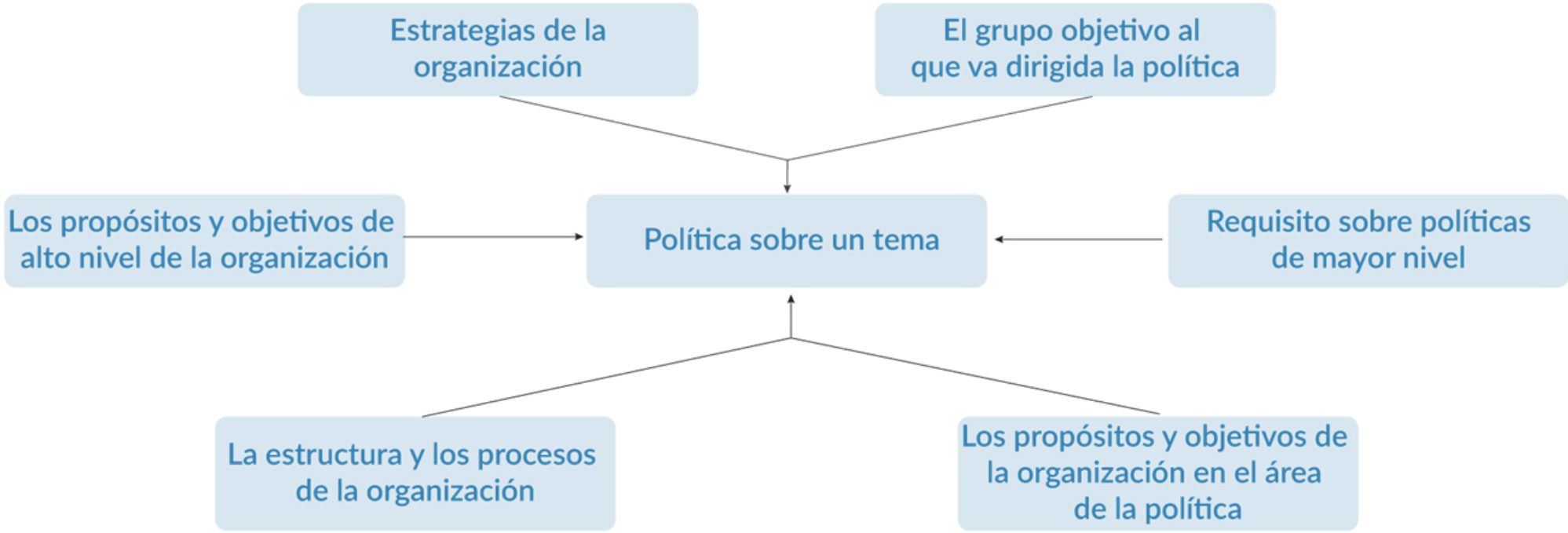
5.2 Políticas – Guía

ISO IEC 27001:2022 requiere que las organizaciones tengan una política de seguridad de la información y especificar cualquier relación particular entre esta política y otras políticas de la organización.

El contenido de las políticas se basa en el contexto en el que opera una organización. Se debe considerar lo siguiente al desarrollar cualquier política dentro del marco de políticas:

1. Las metas y objetivos de la organización;
2. Estrategias adoptadas para lograr los objetivos de la organización;
3. La estructura y los procesos adoptados por la organización;
4. Fines y objetivos asociados al tema de la política;
5. Los requisitos de las políticas relacionadas de nivel superior; y
6. El grupo objetivo al que se dirigirá la política.

5.2 Políticas – Guía



5.2 Políticas – Guía

ESTRUCTURA DE UNA POLÍTICA

Administrativas:

Nombre de la política, versión, fechas de publicación/validez, historia de cambios, dueño(s) y persona(s) que autoriza(n), clasificación, audiencia prevista, etc.

Resumen de la política:

Información general escrita en una o dos oraciones. (Algunas veces puede estar fusionada con la introducción).

Introducción:

Una breve explicación del tema de la política.

Alcance:

Describe aquellas partes o actividades de una organización que son afectadas por la política. Si es pertinente, el alcance enumera las otras políticas que se sustentan en la política.

Objetivos:

Describe la intención de la política.

5.2 Políticas – Guía

ESTRUCTURA DE UNA POLÍTICA

Principios:

Describe las reglas concernientes a las acciones y decisiones para lograr los objetivos. En algunos casos, puede ser útil identificar los procesos.

Responsabilidades:

Describe quién es responsable de las acciones para cumplir los requisitos de la política. En algunos casos, puede incluir una descripción de las disposiciones organizacionales.

Resultados clave:

Describe los resultados del negocio si se cumplen los objetivos. En algunos casos, se pueden fusionar con los objetivos.

Políticas relacionadas:

Describe otras políticas pertinentes al logro de los objetivos, usualmente suministrando detalles adicionales acerca de temas específicos.

Requisitos de la política:

Describe los requisitos detallados de la política.

5.2 Políticas – Guía

POLÍTICAS ESPECÍFICAS

POLÍTICAS	CLÁUSULA
Uso aceptable de la información y otros activos asociados	5.10
Clasificación de la Información	5.12
Transferencia de información	5.14
Control de acceso	5.15
Derechos de acceso	5.18
Seguridad de la información en las relaciones con proveedores	5.19
Seguridad de la información para el uso de servicios en la nube	5.23
Derechos de propiedad intelectual	5.32
Protección de registros	5.33
Privacidad y protección de la PII	5.34
Trabajo Remoto	6.7
Escritorio y Pantalla limpias	7.7
Medios de almacenamiento	7.10
Dispositivos de usuario final	8.1
Derechos de acceso privilegiado	8.2
Restricción de acceso a la información	8.3
Autentificación Segura	8.5

5.2 Políticas – Guía

POLÍTICAS ESPECÍFICAS

POLÍTICAS	CLÁUSULA
Gestión de vulnerabilidades técnicas	8.8
Eliminación de información	8.10
Enmascaramiento de datos	8.11
Respaldo de información	8.13
Inicio de sesión	8.15
Segregación de redes	8.22
Uso de Criptografía	8.24

5.2 Políticas – Metodología

5.2 Políticas – Metodología

Identifique las necesidades internas

LISTADO NECESIDADES INTERNAS	
DIRECCIÓN	
ACCIONISTAS	
EMPLEADOS	

5.2 Políticas – Metodología

Identifique las necesidades externas

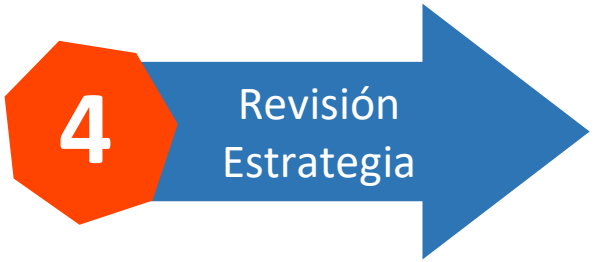
LISTADO NECESIDADES EXTERNAS	
REQUISITOS 27001	
NORMATIVIDAD / LEGISLACIÓN	
FUERZAS DE MERCADO	

5.2 Políticas – Metodología

Establezca el grado de relación que tienen cada una de ellas valorándola en una escala de 1 a 5 (siendo 5 el mayor valor), luego haga sumatorias y los valores más representativos corresponden a directrices o frases que deberían componer la Política

Necesidades	REQUISITOS 27001	NORMATIVIDAD / LEGISLACIÓN	FUERZAS DE MERCADO
DIRECCIÓN			
ACCIONISTAS			
EMPLEADOS			
OTRAS DIRECTRICES			

5.2 Políticas – Metodología



Luego revise visión, misión y otras directrices y determine si hay alguna directriz referente a Seguridad de la información que no ha sido tomada en cuenta, con el fin de incluirla en la política.

Misión

Visión

Principios

5.2 Políticas – Metodología

Recomendaciones para la redacción de una política de seguridad de la información

- La política debe tener como parte de su texto la declaración en la cual se indica ¿qué es lo que se desea hacer?, ¿que regula la política?, ¿cuál es la directriz que deben seguir los funcionarios, contratistas y/o terceros?, todo esto alineado con la estrategia de la organización
- Alinearse con el alcance del SGSI
- Debe especificarse a quién (es) va dirigida la política, se debe identificar fácilmente quién (es) deben cumplir la política
- En caso de que aplique, la política debe indicar las excepciones a la misma y a quiénes les aplica la excepción

5.2 Políticas – Metodología

Recomendaciones para la redacción de una política de seguridad de la información

- En los casos que aplique se hace referencia de la regulación mediante la cual se soporta la política
- Datos de las personas o roles de la entidad que pueden brindar información sobre la política
- Nombre, rol o responsable de quien autoriza la política
- Describir los pasos y procedimientos para realizar ajustes a la política
- Explicación de las consecuencias que se pueden tener en caso de que un funcionario, contratista o tercero incumpla la política
- Fecha que inicia la vigencia de la política

5.2 Políticas - Metodología

Redacción:

Es importante aclarar que una política:

- **NO** es un estándar
- **NO** debe indicar cómo se ejecutará ninguna labor o control de manera específica
- **NO** indica tecnologías específicas de uso

Son declaraciones muy generales y de alto nivel que plasman un objetivo a cumplir por parte de la organización.

5.3 Roles, Responsabilidades y Autoridades Organizacionales – Requisito

La alta dirección debe garantizar que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información son designados y comunicados en toda la organización.

5.3 Roles, Responsabilidades y Autoridades Organizacionales – Explicación

La alta dirección debe garantizar que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información son designados y comunicados en toda la organización.

El propósito de este requisito es asignar responsabilidades y autoridades para asegurar la conformidad del SGSI con los requisitos de ISO IEC 27001:2022 y para garantizar la presentación de informes sobre el desempeño del SGSI a la alta dirección.

5.3 Roles, Responsabilidades y Autoridades Organizacionales – Guía

La alta dirección debe garantizar periódicamente que las responsabilidades y autoridades del SGSI sean asignados para que el sistema de gestión cumpla con los requisitos establecidos en la norma ISO IEC 27001:2022.

No es necesario asignar todos los roles, responsabilidades y autoridades, pero debe hacerlo adecuadamente al delegar autoridad para hacer esto.

La alta dirección debe aprobar los principales roles, responsabilidades y autoridades del SGSI.

5.3 Roles, Responsabilidades y Autoridades Organizacionales – Guía

Se deberían asignar las **responsabilidades** y las **autoridades** con las siguientes actividades de seguridad de la información

- Coordinar el establecimiento, implementación, mantenimiento, reporte de desempeño y mejora del SGSI.
- Asesorar con relación a la valoración y tratamiento de riesgos de seguridad de la información.
- Diseñar procesos y sistemas de seguridad de la información.
- Establecer estándares acerca de la determinación, configuración y operación de controles de seguridad de la información.
- Gestionar los incidentes de seguridad de la información.
- Revisar y auditar el SGSI.

5.3 Roles, Responsabilidades y Autoridades Organizacionales – Guía

Responsabilidades y autoridades de seguridad de la información pertinentes que se deberían incluir dentro de otras funciones.

Por Ejemplo, las responsabilidades de seguridad de la información se pueden incorporar en los roles de:

- Dueños de la información
- Dueños de procesos
- Dueños de activos (por ejemplo, dueños de aplicaciones o de infraestructura)
- Dueños de riesgos
- Las funciones o personas que coordinan la seguridad de la información (este rol particular normalmente es un rol de soporte en el SGSI)
- Gerentes de proyecto
- Gerentes de línea
- Usuarios de información

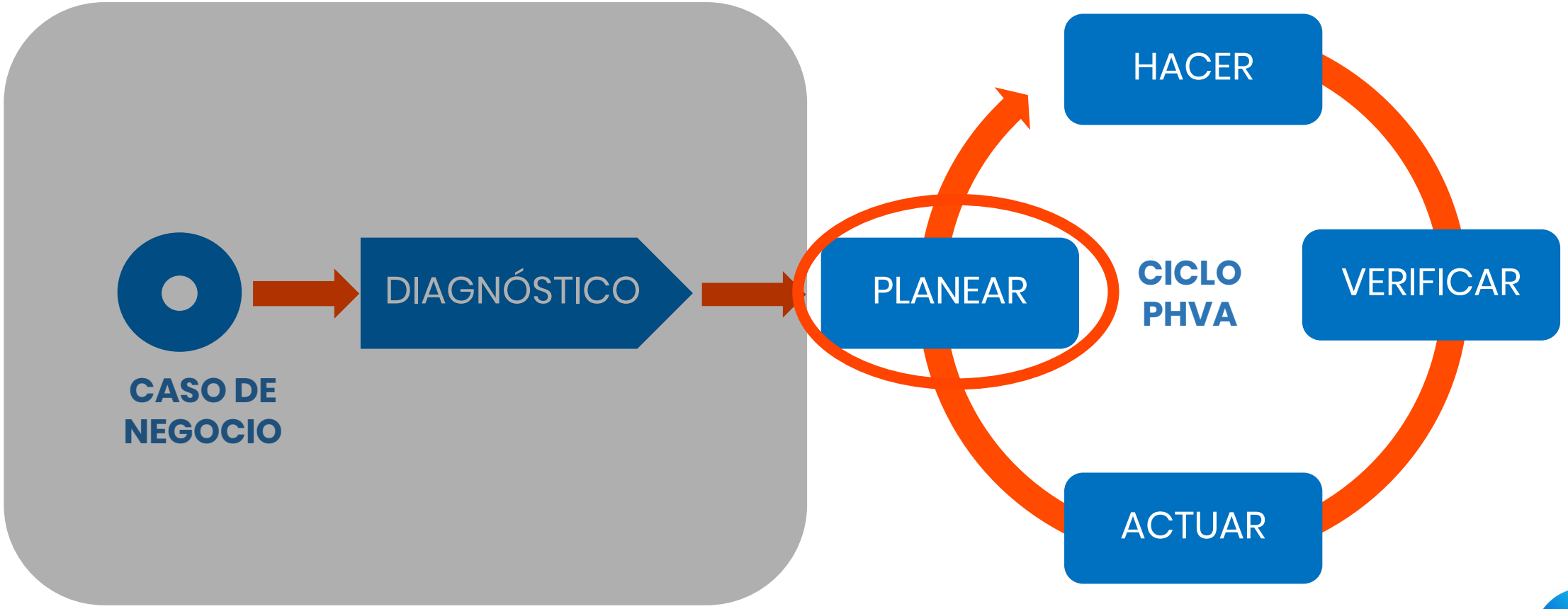
La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y medida que la organización considere necesaria para la eficacia de su sistema de gestión.

6. Planificación: Interpretar los Requisitos de ISO IEC 27001

6.1 Acciones para Tratar Riesgos y Oportunidades.
6.1.2 Evaluación de riesgos de SI.
6.1.3 tratamiento de riesgos de SI.
6.2 Objetivos de Seguridad de la Información.

Objetivo de la ruta de navegación

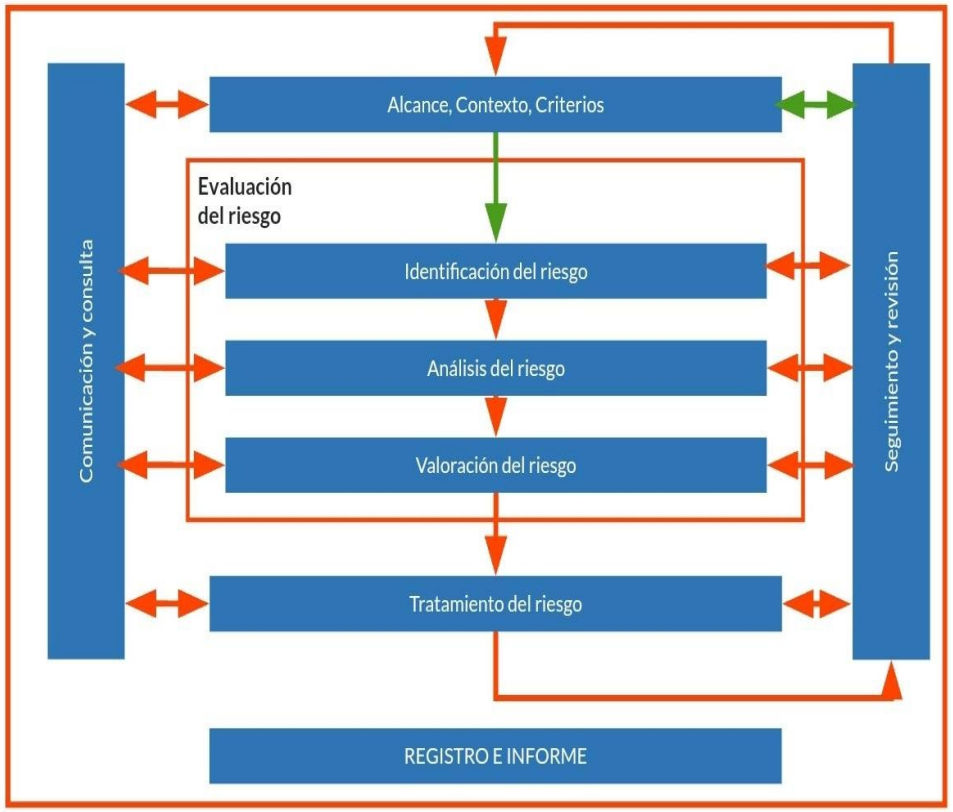
El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (Planear) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de diseñar y aplicar un modelo de gestión de riesgos.

También es importante que el ISO IEC 27001:2022 Implementador Líder esté en capacidad de incluir en su trabajo una valoración de riesgos y planeación de tratamiento de riesgos.



Estructura de ISO IEC 27001

Requisitos y cómo abordarlos

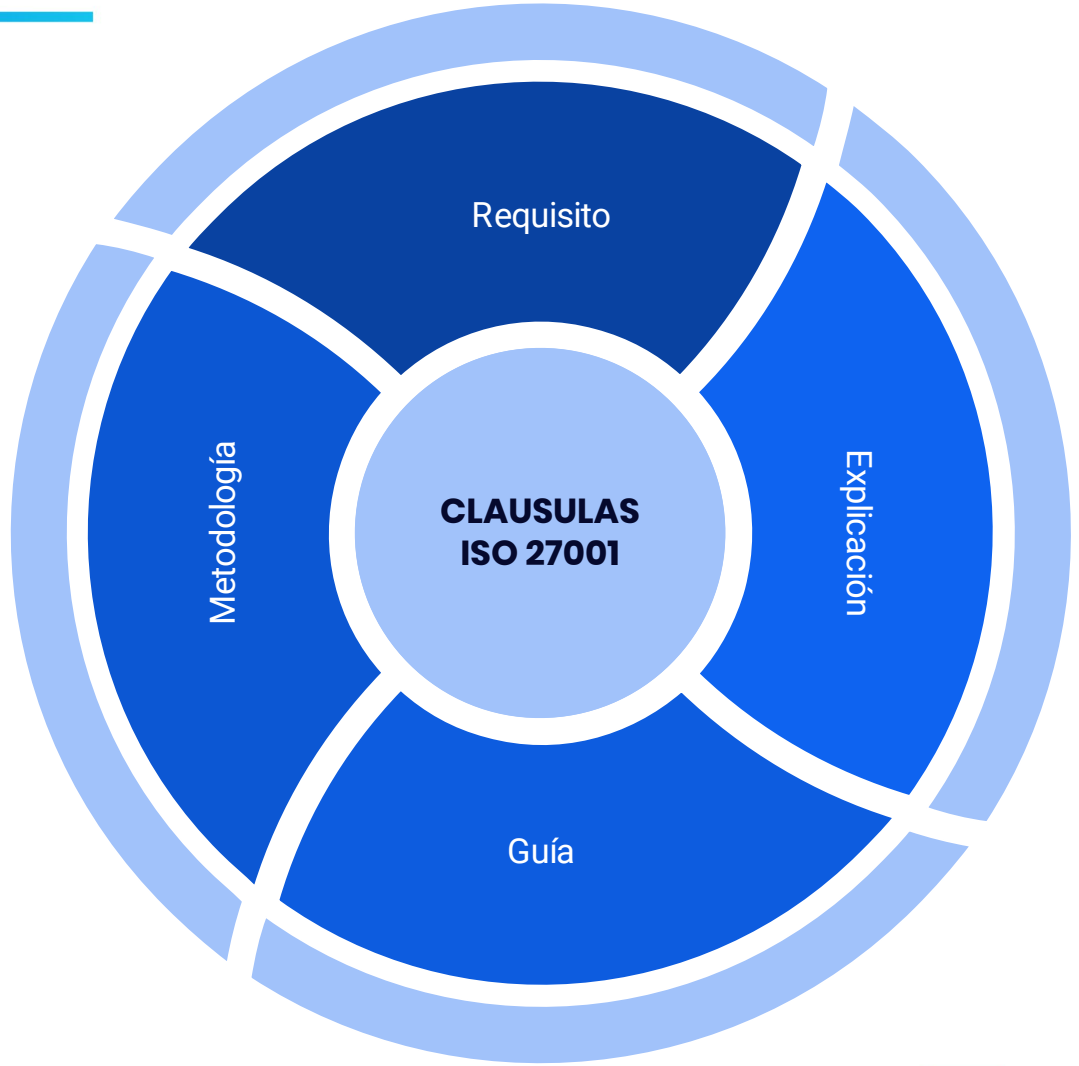
En este módulo se abordan los requisitos declarados en la cláusula 6 de la ISO IEC 27001:2022 desde 4 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 6 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Metodología: Serie de métodos, técnicas, mejores prácticas y pasos recomendados para abordar los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarados en la cláusula 6 de la ISO 27001 (se incluye para el tema definido en el alcance del módulo).



6.1 Acciones para Tratar Riesgos y Oportunidades

6.1 Acciones para Tratar Riesgos y Oportunidades

La ISO IEC 27001:2022 en su cláusula 6.1 se ocupa de la planificación de acciones para abordar todo tipo de riesgos y oportunidades que son relevantes para el SGSI, esto incluye la evaluación de riesgos y la planificación de riesgos y su tratamiento.

La estructura de la ISO IEC 27001:2022 subdivide los riesgos en dos categorías durante la planificación:
a) riesgos y oportunidades relevantes para los resultados previstos del SGSI en su conjunto; y
b) riesgos de seguridad de la información que se relacionan con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI.

La primera categoría debe manejarse de acuerdo con los requisitos especificados en la ISO IEC 27001:2022, cláusula 6.1.1. Los riesgos que entran en esta categoría pueden ser riesgos relacionados con el propio SGSI, el alcance del SGSI, el compromiso de la alta dirección con la seguridad de la información, los recursos para operar el SGSI,

Las oportunidades que caen en esta categoría pueden ser oportunidades relacionadas con los resultados del SGSI, el valor comercial de un SGSI, la eficiencia de los procesos e información operativos del SGSI, controles de seguridad, etc.

6.1 Acciones para Tratar Riesgos y Oportunidades

La segunda categoría consiste en todos los riesgos que se relacionan directamente con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI. Estos riesgos deben manejarse de acuerdo con la cláusula 6.1.2 (evaluación de riesgos de seguridad de la información) y 6.1.3 (tratamiento de riesgos de seguridad de la información).

Las organizaciones pueden optar por utilizar diferentes técnicas para cada categoría, la subdivisión de requisitos para abordar los riesgos se puede explicar de la siguiente manera:

- Fomenta la compatibilidad con otros estándares de sistemas de gestión para esas organizaciones que cuentan con sistemas de gestión integrados para diferentes aspectos como calidad, medio ambiente y seguridad de información;
- Requiere que la organización defina y aplique procesos completos y detallados para la información, evaluación y tratamiento de riesgos de seguridad; y
- Enfatiza que la gestión de riesgos de seguridad de la información es el elemento central de un SGSI.

6.1 Acciones para Tratar Riesgos y Oportunidades – Requisito

Al planificar el SGSI, la organización determina los riesgos y oportunidades considerando cuestiones mencionadas en 4.1 y requisitos mencionados en 4.2.

RISK

6.1 Acciones para Tratar Riesgos y Oportunidades – Explicación

La organización planifica su SGSI para:

a) Garantizar que el SGSI entregue los resultados previstos, que los riesgos de seguridad de la información sean conocidos por los propietarios del riesgo y tratados a un nivel aceptable;

Los riesgos relacionados podrían ser procesos y responsabilidades poco claros, falta de conciencia entre empleados, falta de compromiso por parte de la dirección, etc.

b) Prevenir o reducir los efectos no deseados de los riesgos relevantes para los resultados previstos del SGSI; y

Los riesgos relacionados podrían ser riesgos de deficiente gestión o escasa conciencia de los riesgos.

c) Lograr una mejora continua (ver 10.2), mediante mecanismos adecuados para detectar y corregir debilidades en los procesos de gestión o aprovechar oportunidades de mejora en la seguridad de información.

Los riesgos relacionados podrían ser una mala gestión de la documentación y procesos del SGSI.

6.1 Acciones para Tratar Riesgos y Oportunidades - Explicación

Cuando una organización busca oportunidades en sus actividades, estas actividades afectan el contexto de la organización (cláusula 4.1) o las necesidades y expectativas de las partes interesadas (cláusula 4.2), y puede cambiar los riesgos para la organización.

Ejemplos de tales oportunidades puede ser: centrar su negocio en algunas áreas de productos o servicios, establecer una estrategia de marketing para algunas regiones geográficas, o ampliar asociaciones comerciales con otras organizaciones.

También existen oportunidades en la mejora continua de los procesos y la documentación del SGSI, junto con la evaluación de los resultados previstos entregados por el SGSI. Por ejemplo, la consideración de un SGSI relativamente nuevo a menudo da como resultado la identificación de oportunidades para refinar los procesos al aclarar interfaces, reduciendo la sobrecarga administrativa, eliminando partes de los procesos que no son rentables, perfeccionando la documentación e introduciendo nuevas tecnologías de la información.

La planificación incluye la determinación de
-Acciones para abordar los riesgos y oportunidades; y
-La forma de integrar e implementar estas acciones en los procesos del SGSI; y evaluar la efectividad de estas acciones.

6.1 Acciones para Tratar Riesgos y Oportunidades - Guía

La organización debería:

Determinar riesgos y oportunidades que pueden afectar el logro de las metas considerando las cuestiones mencionadas en 4.1 y los requisitos mencionados en 4.2; y desarrollar un plan para implementar las acciones determinadas y evaluar su efectividad.

Las acciones deben planificarse considerando la integración de los procesos de seguridad de la información.
y documentación en estructuras existentes; todas estas acciones están vinculadas con la seguridad de la información contra los cuales se evalúan y tratan los riesgos de seguridad de la información.

Las acciones requeridas pueden ser diferentes para niveles estratégicos, tácticos y operativos, para diferentes sitios, o para diferentes servicios o sistemas.

Se pueden adoptar varios enfoques:
—Considerar los riesgos y oportunidades asociados con la planificación, implementación y operación del SGSI por separado de los riesgos de seguridad de la información; y
— Considerar todos los riesgos simultáneamente.

6.1 Acciones para Tratar Riesgos y Oportunidades - Guía

Una organización que está integrando un SGSI en un sistema de gestión establecido puede encontrar que los requisitos de 6.1.1 se cumplen mediante la metodología de planificación empresarial existente de la organización.

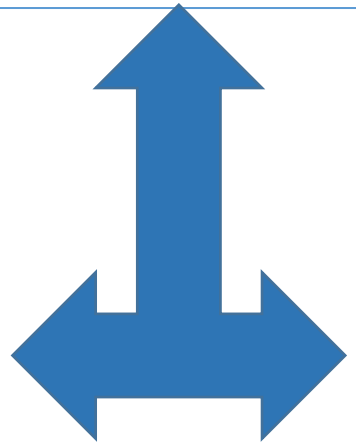
Si este es el caso, se debe tener cuidado de verificar que la metodología cubra todos los requisitos.

La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y medida que la organización considere necesaria para la eficacia de su sistema de gestión.

6.1 Acciones para Tratar Riesgos y Oportunidades – Metodología

Establecer el contexto de la organización.
La Organización articula sus objetivos y define componentes externas e internas a considerar para establecer el alcance y los criterios de desempeño del riesgo.

Condiciones externas e internas que podrían generar impactos en el cumplimiento de los objetivos.



Externo
- Ambiente social y cultural
- Entorno político
- Cumplimiento, legal y reglamentaria
- Tecnología
- Entorno económico
- Competitividad
- Impulsores

Interno
- Cultura Organizacional
- Gobierno, estructura, funciones y responsabilidades
- Normas, directrices, procesos
- Componentes técnicos
- Tecnología Interna
- Clientes
- Aspectos sociales

6.1.2 Evaluación de los riesgos de S.I. - Requisito

La organización define y aplica un **proceso de evaluación de riesgos de seguridad de la información**

RISK

6.1.2 Evaluación de los riesgos de S.I. - Explicación

La organización define y aplica un **proceso de evaluación de riesgos de seguridad de la información** que:

a) establece y mantiene
1) los criterios de aceptación del riesgo; y
2) criterios para realizar evaluaciones de riesgos de seguridad de la información, que pueden incluir criterios de evaluación de las consecuencias y probabilidad, y reglas para la determinación del nivel de riesgo; y

b) garantiza que las evaluaciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y resultados comparables.

El proceso de evaluación de riesgos de seguridad de la información se define luego a lo largo de los siguientes subprocesos:

c) identificación de riesgos de seguridad de la información:
1) identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad para información dentro del alcance del SGSI; y
2) identificar a los propietarios de los riesgos asociados con estos riesgos, es decir, identificar y nombrar personas con la autoridad y responsabilidad apropiadas para gestionar los riesgos identificados.

6.1.2 Evaluación de los riesgos de S.I. - Explicación

d) análisis de los riesgos de seguridad de la información:

1) evaluar las posibles consecuencias en caso de que los riesgos identificados se materialicen como pérdidas monetarias o impactos comerciales indirectos como daños a la reputación. Las consecuencias evaluadas se pueden informar con valores cuantitativos o cualitativos;

2) evaluar la probabilidad realista de ocurrencia de los riesgos identificados, con análisis cuantitativos (es decir, probabilidad o frecuencia) o valores cualitativos; y

3) determinar los niveles de riesgo identificados como una combinación predefinida de consecuencias evaluadas y probabilidades evaluadas; y

e) evaluación de los riesgos de seguridad de la información:

1) comparar los resultados del análisis de riesgos con los criterios de aceptación de riesgos establecidos anteriormente; y

2) priorizar los riesgos analizados para el tratamiento de riesgos, es decir, determinar la urgencia del tratamiento de los riesgos que se consideran inaceptables y secuenciar si varios riesgos necesitan tratamiento.

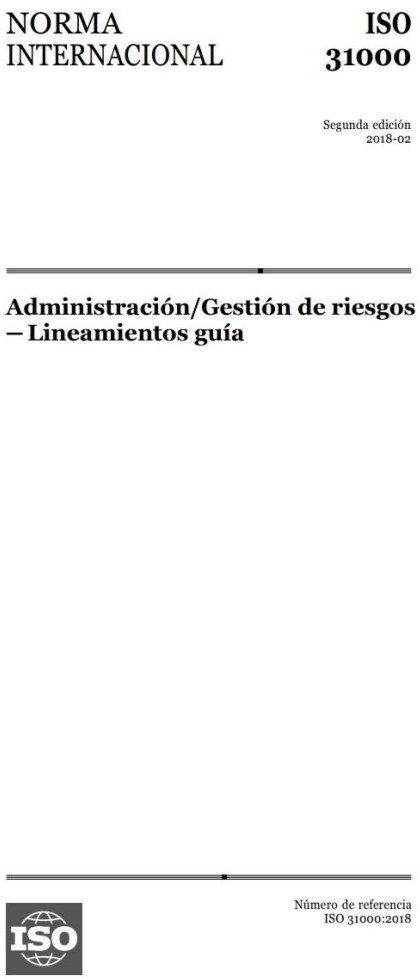
Al aplicar **el proceso de evaluación de riesgos** de seguridad de la información, todos los pasos, así como los resultados de su aplicación se conserva como información documentada.

6.1.2 Evaluación de los riesgos de S.I. - Guía

Buscando eficiencia y eficacia de los procesos, un **proceso de gestión de riesgos** cuenta con estas características y principios:

- Crea y protege el valor, pues contribuye al logro de los objetivos
- La gestión del riesgo es parte integral de todos los procesos
- Sus salidas son fundamentales en la toma de decisiones
- Se ocupa de la incertidumbre
- Es sistemática, estructurada y oportuna
- Se basa en la mejor información disponible
- Es específica
- Toma en cuenta los factores humanos y culturales de la Organización
- Es transparente e inclusiva pues se ubica en todos los procesos
- Es dinámica, iterativa y orientada al cambio
- Facilita la mejora continua

Recomendación


NORMA INTERNACIONAL

ISO 31000

Segunda edición
2018-02

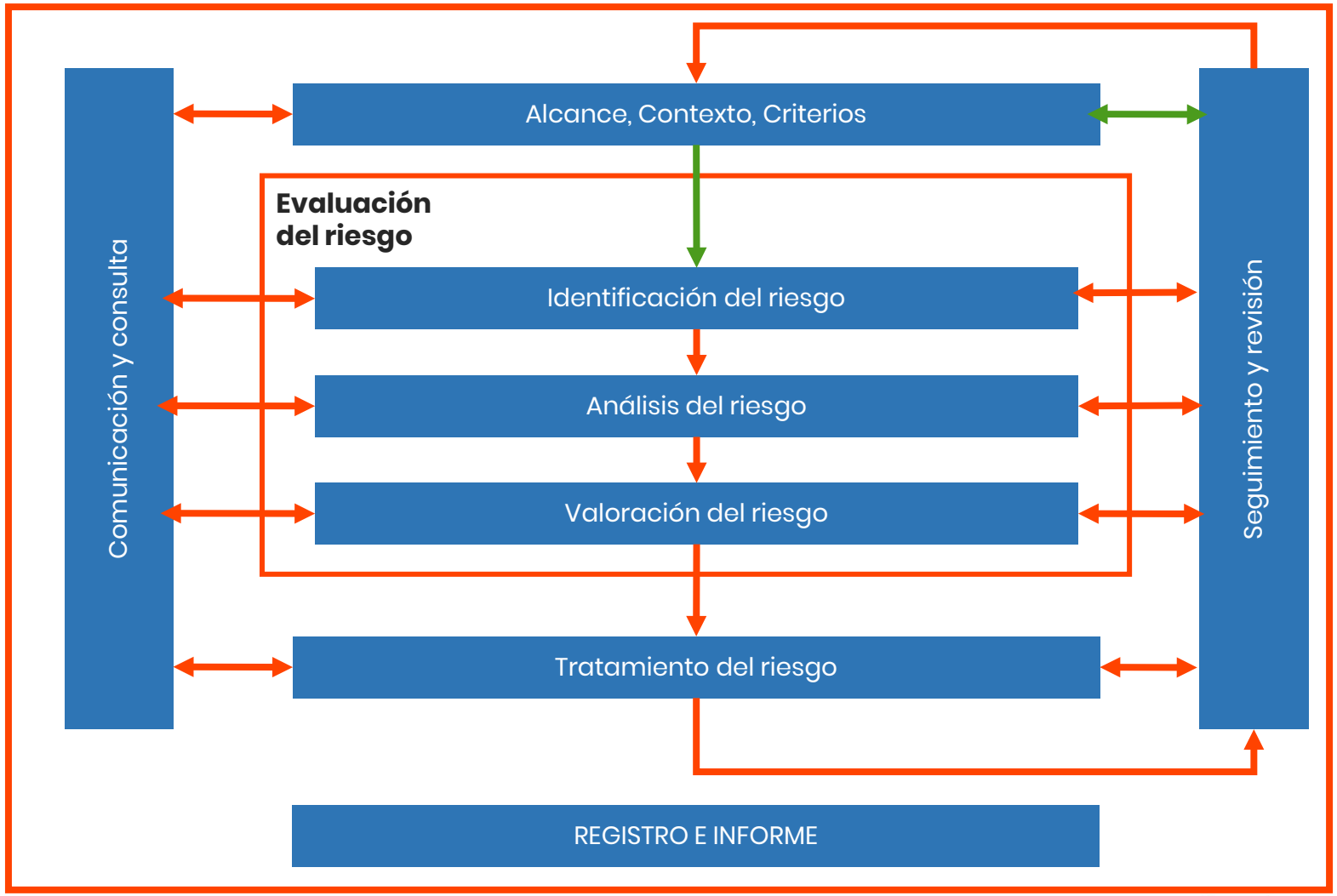
Administración/Gestión de riesgos – Lineamientos guía

Número de referencia
ISO 31000:2018

Se recomienda consultar la norma ISO 31000:2018 para mayor orientación sobre el modelo de gestión de riesgos adoptado por la ISO 27001:2022.

6.1.2 Evaluación de los riesgos de S.I. - Guía

Proceso de evaluación de riesgos basado en la ISO 31000



6.1.2 Evaluación de los riesgos de S.I. - Guía

Orientación sobre el establecimiento de criterios de riesgo.

Los criterios de riesgos de seguridad de la información deben establecerse considerando el contexto de la organización y los requisitos de las partes interesadas deben definirse de acuerdo con las recomendaciones de la alta dirección.

Los criterios de riesgo de seguridad de la información deben establecerse en relación con los resultados previstos del SGSI según la norma ISO/IEC 27001:2022, 6.1.2 a), criterios relativos a la evaluación de riesgos de seguridad de la información.

Se deben establecer criterios considerando:
La evaluación de probabilidad y consecuencias.
Establecer criterios de aceptación.

Después de establecer criterios para evaluar las consecuencias y probabilidades de seguridad de la información la organización también debe establecer un método para combinarlos con el fin de determinar un nivel de riesgo.

6.1.2 Evaluación de los riesgos de S.I. - Guía

Las consecuencias y probabilidades pueden expresarse de forma cualitativa, cuantitativa o semi-cuantitativa

Los criterios de aceptación de riesgos se relacionan con la evaluación de riesgos (en su fase de evaluación, cuando la organización debe entender si un riesgo es aceptable o no), y las actividades de tratamiento de riesgos (cuando la organización debe entender si el tratamiento de riesgo propuesto es suficiente para alcanzar un nivel de riesgo aceptable).

Los criterios de aceptación de riesgos **pueden basarse en un nivel máximo de riesgos aceptables,** en costos-beneficios y consideraciones o consecuencias para la organización.

Los criterios de aceptación de riesgos deben ser aprobados por la dirección responsable.

Orientación sobre cómo producir resultados de evaluación consistentes, válidos y comparables (6.1.2 b)

El proceso de evaluación de riesgos debe basarse en métodos y herramientas diseñados con suficiente detalle para que produzcan resultados consistentes, válidos y comparables.

6.1.2 Evaluación de los riesgos de S.I. - Guía

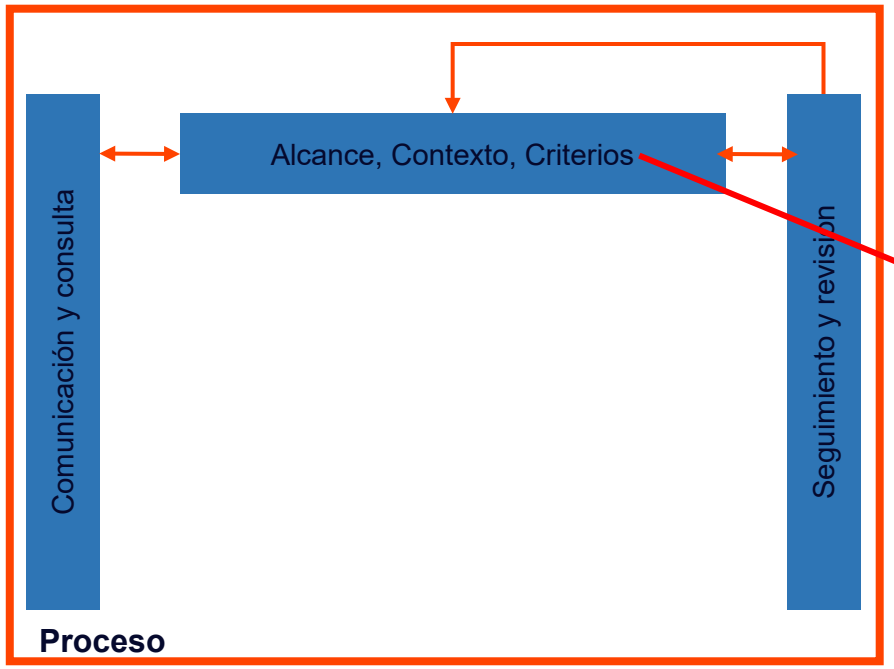
Cualquiera que sea el método elegido, el proceso de evaluación de riesgos de seguridad de la información debe garantizar que:

— Se consideran todos los riesgos, con el nivel de detalle necesario;

— Sus resultados sean consistentes y reproducibles (es decir, la identificación de riesgos, su análisis y su evaluación puede ser entendida por un tercero y los resultados son los mismos cuando diferentes personas evalúan los riesgos en el mismo contexto); y

— Los resultados de evaluaciones de riesgos repetidas son comparables (es decir, es posible entender si los niveles de riesgo aumentan o disminuyen).

6.1.2 Evaluación de los riesgos de S.I. - Metodología



- Considerando el contexto de la organización, cláusula 4.1
- Considerando el alcance del SGSI.
- Considerando las partes interesadas y sus Requisitos, cláusula 4.2.
- Establecer criterios para evaluar las consecuencias y probabilidades de seguridad de la información.
- Establecer un método para combinarlos con el fin de determinar un nivel de riesgo.
- Expresar el nivel del riesgo de forma cualitativa, cuantitativa o semi-cuantitativa.
- Establecer el nivel del riesgo Máximo aceptable.
- Deben ser autorizados por la dirección.

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Establecer criterios para evaluar las consecuencias y probabilidades de seguridad de la información.

Tabla de Probabilidad / Frecuencia		
Nivel	Rangos	Ejemplo Detallado de la Descripción
1	Muy Poco Probable	Puede ocurrir solo bajo circunstancias excepcionales
2	Poco Probable	Podría ocurrir algunas veces (Pocas veces)
3	Probable	Puede ocurrir en algún momento
4	Bastante Probable	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	Muy Probable	La expectativa de ocurrencia se de en la mayoría de las circunstancias
Tabla de impacto: Prioridad 1 – Impacto en la Operación		
Nivel	Rangos	Ejemplo Detallado de la Descripción
1	Sin Impacto	Hay una indisponibilidad menor o igual a 5 minutos
2	Muy Bajo	Hay una indisponibilidad entre 6 y 15 minutos
3	Bajo	Hay una indisponibilidad entre 15 y 30 minutos
4	Moderado	Hay una indisponibilidad entre 30 y 60 minutos
5	Alto	Hay una indisponibilidad por mayor a 60 minutos. Es necesario un establecer un mecanismo de procesamiento alterno

Priorizar los riesgos según su gravedad. Es decir, cuanto mayor sea la probabilidad y mayor sea el impacto, mayor ha de ser la **prioridad** de gestión y de respuesta.

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Establecer un método para combinarlos con el fin de determinar un nivel de riesgo.

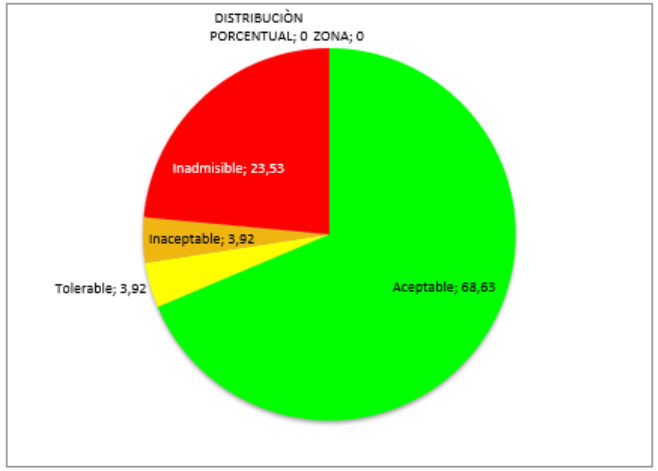
Matriz resultante del CRUCE Probabilidad X Impacto

MAPA DE RIESGOS

Probabilidad		Impacto				
	valor	Insignificante	Menor	Moderado	Mayor	Catastrofico
		1	2	3	4	5
Casi seguro	5					
Probable	4					ATAQUES INFORMÁTICOS -- ALMACENAMIENTO || ATAQUES INFORMÁTICOS -- SERVIDOR F_E || ATAQUES INFORMÁTICOS -- CONOCIMIENTO NEGOCIO || COMPROMISO DE LA INFORMACIÓN -- CONOCIMIENTO NEGOCIO ||
Posible	3		PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL || PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO ||		COMPROMISO DE LAS FUNCIONES -- CONOCIMIENTO NEGOCIO ||	ACCIONES NO AUTORIZADAS -- CONOCIMIENTO NEGOCIO || COMPROMISO DE LA INFORMACIÓN -- DOMINA DIGITAL F_E || COMPROMISO DE LA INFORMACIÓN -- SOFTWARE GESTION F_E ||
Improbable	2	ACCIONES NO AUTORIZADAS -- REDES ||	EVENTO NATURAL -- REDES || PERDIDA DE SERVICIOS ESCENCIALES -- REDES || FALLAS TECNICAS -- REDES || FALLAS TECNICAS -- SERVIDOR LOCAL || FALLAS TECNICAS -- EQUIPO DE CÓMPUTO || FALLAS TECNICAS -- EQUIPO MÓVIL || DAÑO FÍSICO -- SERVIDOR LOCAL || DAÑO FÍSICO -- EQUIPO DE CÓMPUTO || DAÑO			FALLAS TECNICAS -- DOMINA DIGITAL F_E || FALLAS TECNICAS -- SOFTWARE GESTION F_E || PERSONAL NO SATISFECHO -- DOMINA DIGITAL F_E || PERSONAL NO SATISFECHO -- CONOCIMIENTO NEGOCIO ||
Raro	1	EVENTO NATURAL -- INFORM. FÍSICA 1 || EVENTO NATURAL -- INFORM. FÍSICA 2 || DAÑO	EVENTO NATURAL -- EQUIPO DE CÓMPUTO || DAÑO FÍSICO -- REDES ||			DAÑO FÍSICO -- ALMACENAMIENTO || DAÑO FÍSICO -- SERVIDOR F_E ||

Muestra gráfica del estado de los procesos

ZONA	%	Total riesg
DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesg
Aceptable	68,63	35
Tolerable	3,92	2
Inaceptable	3,92	2
Inadmisible	23,53	12
		51



6.1.2 Evaluación de los riesgos de S.I. – Guía

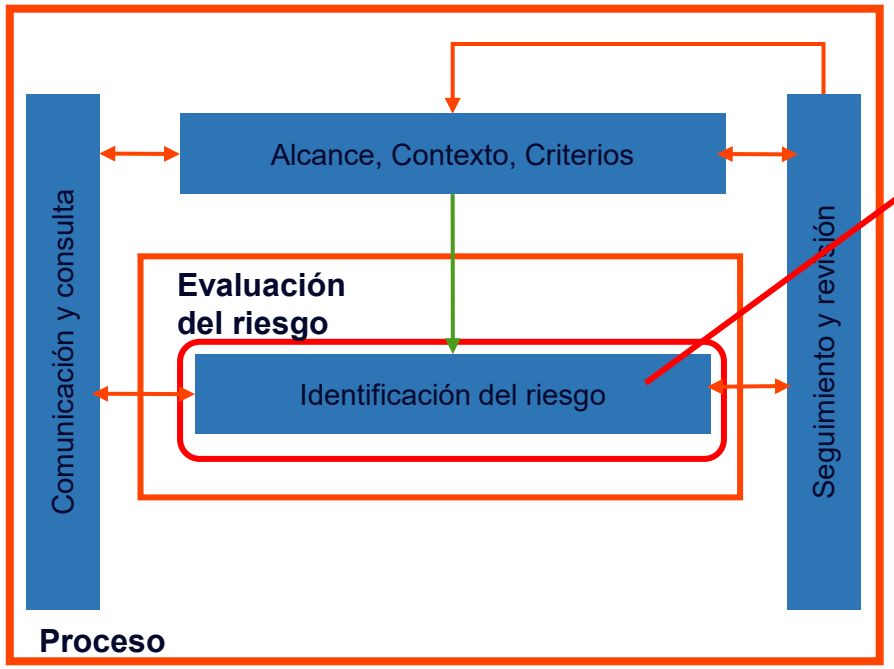
Orientación sobre la identificación de riesgos de seguridad de la información.

La identificación de riesgos es el proceso de encontrar, reconocer y describir riesgos. Esto involucra el identificación de fuentes de riesgo, eventos, sus causas y sus posibles consecuencias.

El objetivo de la identificación de riesgos es generar una lista completa de riesgos basada en aquellos eventos que
podría crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos de la seguridad de la información.

Normalmente se utilizan dos enfoques para la identificación de riesgos de seguridad de la información:
— Enfoque basado en eventos: considera las fuentes de riesgo de forma genérica. Los hechos considerados pueden haber ocurrido en el pasado o pueden anticiparse para el futuro, en el primer caso pueden involucrar datos históricos, en el segundo caso pueden basarse en análisis teóricos y opiniones de expertos; y
— Enfoque basado en la identificación de activos, amenazas y vulnerabilidades: considera dos tipos diferentes de fuentes de riesgo: activos con sus vulnerabilidades intrínsecas y amenazas. Eventos potenciales considerados
Aquí hay formas de cómo las amenazas podrían explotar una cierta vulnerabilidad de un activo para impactar el objetivos de la organización.

6.1.2 Evaluación de los riesgos de S.I. - Metodología



Por lo general se usan dos enfoques para la identificación de los riesgos de seguridad de la información:

- **Enfoque basado en eventos** y/o **Enfoque basado en la identificación de activos, amenazas y vulnerabilidades.**

El enfoque basado en activos, amenazas y vulnerabilidades corresponde al enfoque de seguridad de la información.

El enfoque de identificación de riesgos compatible con los requisitos de ISO/IEC 27001 para garantizar que las inversiones en identificación de riesgos no se pierdan.

No se recomienda que la identificación de riesgos sea demasiado detallada en el primer ciclo de evaluación de riesgos.

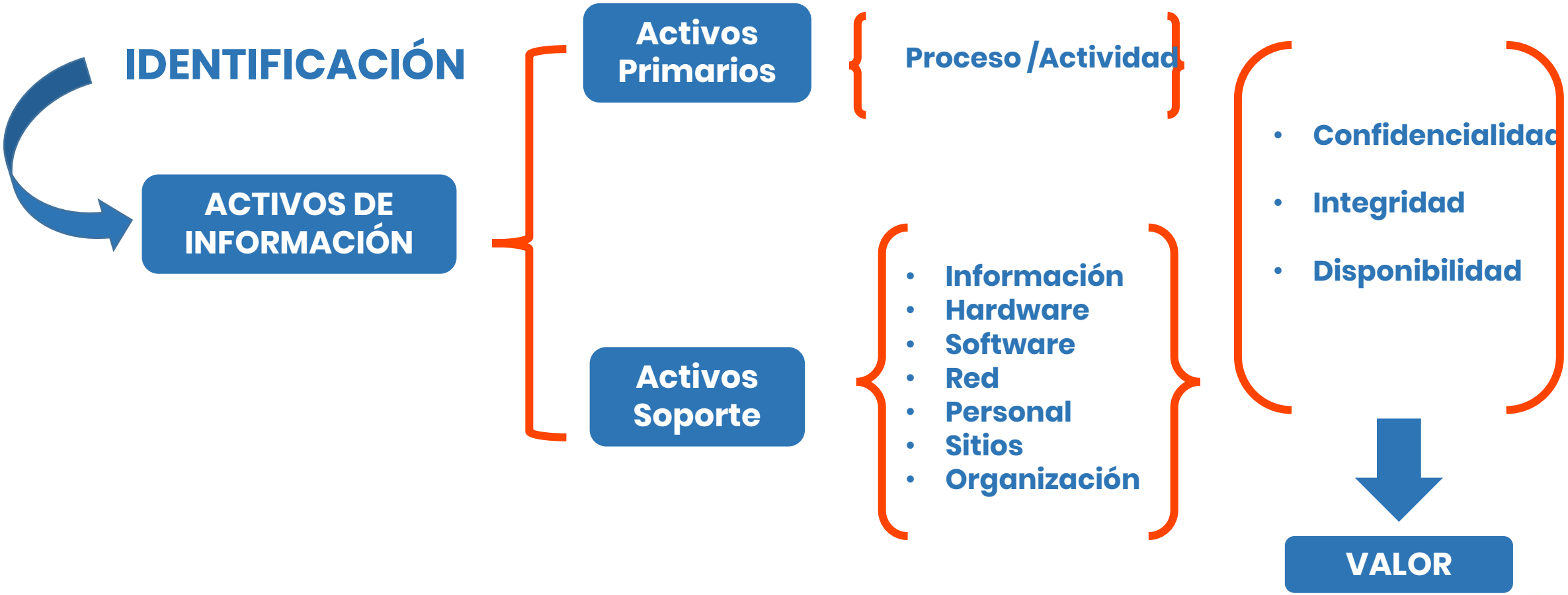
6.1.2 Evaluación de los riesgos de S.I. - Metodología

Identificación de activos para el enfoque basado en activos, amenazas y vulnerabilidades.

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

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

6.1.2 Evaluación de los riesgos de S.I. - Metodología



6.1.2 Evaluación de los riesgos de S.I. - Metodología

Clasificación de activos

Resumen			
Ítem	**Código**	**Clasificación**	**Tipo**
1	IF1	Información Física 1	Documental
2	IF2	Información Física 2	
3	S1	Herramientas para la Operación	Software
4	S2	Software Gestión	
5	R1	Red	Infraestructura
6	SL	Servidor Local	
7	EC	Equipo de computo	Equipos
8	AL	Almacenamiento.	Almacenamiento
9	CN	Conocimiento del negocio	Intangible y RH

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Amenaza

Están presentes en cada sistema o activo bajo las premisas de:

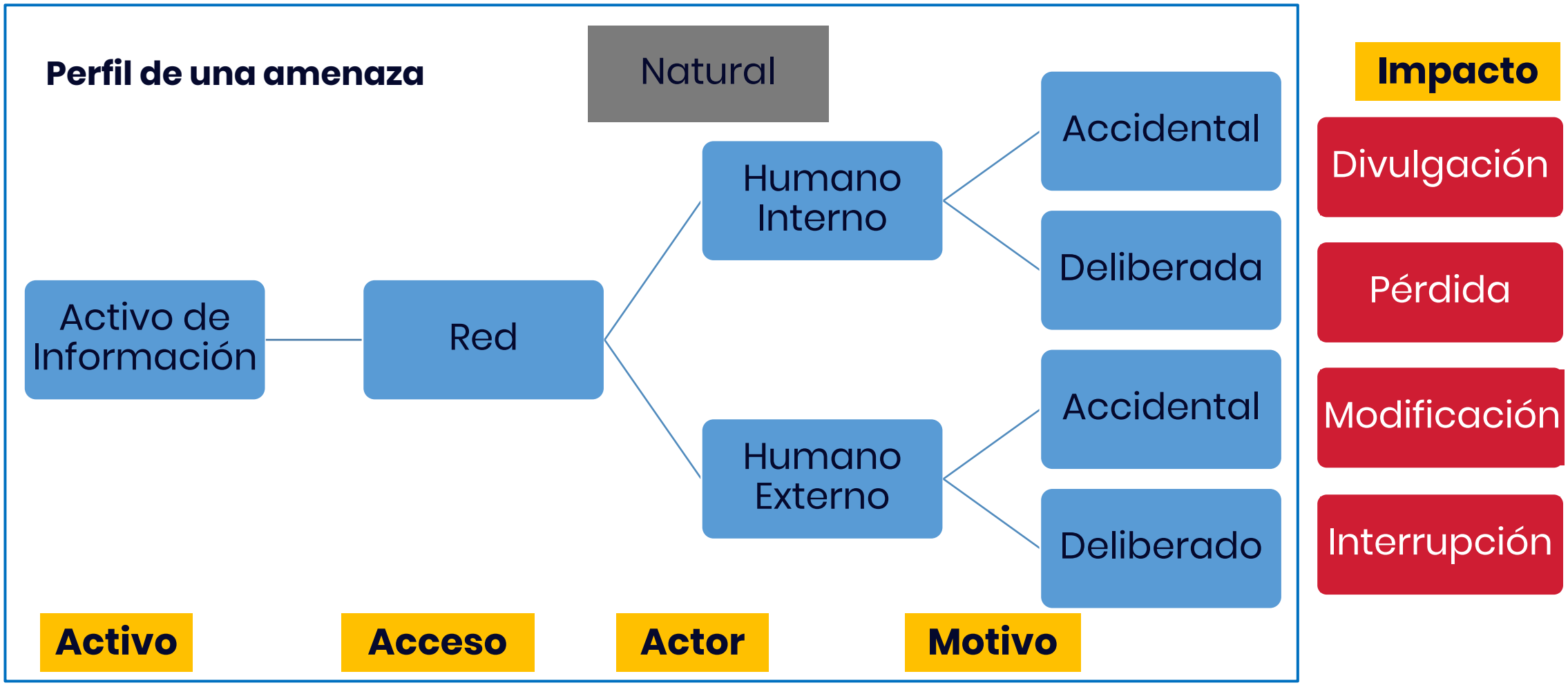
- Confidencialidad
- Disponibilidad
- Integridad

El propósito es reducir el impacto negativo. De naturaleza defensiva.

Escenario (Causa) donde una acción o suceso (incidente) compromete la seguridad de un Activo de Información.

Causa: Motivo o circunstancia.

6.1.2 Evaluación de los riesgos de S.I. - Metodología



6.1.2 Evaluación de los riesgos de S.I. - Metodología

CLASIFICACIÓN Y VALORACIÓN → **ACTIVOS DE INFORMACIÓN**

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN		CONFIDENCIALIDAD			INTEGRIDAD			DISPONIBILIDAD			CONSOLIDADO DE VALORACIÓN			TOTAL
N. ACTIVO	NOMBRE DEL ACTIVO	FINANCIERO	JURÍDICO	IMAGEN	FINANCIERO	JURÍDICO	IMAGEN	FINANCIERO	JURÍDICO	IMAGEN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
1	Activo 1													

6.1.2 Evaluación de los riesgos de S.I. – Metodología

Clasificación de amenazas y vulnerabilidades a los activos de información

AMENAZAS TIC	
Interceptación	COMPROMISO DE LA INFORMACIÓN
Espionaje	
Pérdida / Hurto de medios o equipos	
Recuperación de medios	
Divulgación	
Fuentes de datos no confiables	
Incumplimiento obligaciones legales	
Detección de ubicación	
Abuso tecnológico, Operaciones indebidas con los equipos y aplicativos.	ACCIONES NO AUTORIZADAS
Uso no autorizado del equipo	
Copia del software	
Uso de software ilegal	
Corrupción base de los datos	
Procesamiento ILEGAL de datos	
Error en el uso / bloqueo equipo	COMPROMISO DE LAS FUNCIONES
Abuso de los derechos	
Incumplimiento de terceros	
Suplantación de identidad	
Incumplimiento de funciones	
DDOS	ATAQUES INFORMÁTICOS
Cross Site Scripting (XSS)	
Inyección SQL	
Desbordamiento de buffer	
Fuerza Bruta	
Exploits	
Malware	
Puertas traseras	
Ciberestafas	
Energia electrica	PERDIDA DE SERVICIOS ESCENCIALES
Agua o aire acondicionado	
Falla de la RED	

VULNERABILIDADES
Falta de segregación de roles
Configuracion incorrecta de sistemas de información
Falta de capacitacion de usuarios
Vulnerabilidades de dia cero
Fallas por falta de capacitación operadores
Enfermedades
Fallas por actualizaciones
Desconocimiento de herramientas
Falta de compromiso de la alta direccion
Ausencia de estándares para definir criterios o tipología de eventos que podrían generar riesgos a la seguridad de la red del cliente.
La persona no identifica un ataque en la red
Incapacidad de ejecución de tareas por el desequilibrio de carga laboral y/o gestión de capacidad (por tiempo).
Ausencia de un estándar de desarrollo que permita elegir los nuevos comportamientos a detectar por medio del IDS o de escaneo inicial realizado en el proceso de registro.
NO se detectan dispositivos con fallas físicas o de configuración
Errores en configuración que no permiten encendido remoto

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Ejemplos de amenazas a la información:

- Daño físico (Contaminación, accidentes, fuego, etc.)
- Introducción de código malicioso al sistema
- Accesos/cambios no autorizados
- Ilegalidad de software
- Fraudes /robos de identidad
- Pérdida inesperada de los servicios críticos
- Accidentes ocasionados por eventos de la naturaleza

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Vulnerabilidad.

Dejan a un sistema expuesto al ataque de una amenaza o permite el éxito o mayor impacto de la amenaza. Son explotadas por las amenazas.

Ej.: Incendio por Gas.

Ineficiencia, condiciones adversas de operación, reputación, pérdida de oportunidad se identifican como consecuencias de las vulnerabilidades.

Grado de sensibilidad de un Activo.

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Las **Vulnerabilidades son** Debilidades de cualquier tipo que compromete la seguridad de un Sistema de Información.

- Aplicativos con defectos de construcción sin testing
- Configuraciones defectuosas en redes y equipos
- Ausencia de política de Continuidad de las operaciones
- Desactualización del Sistema Operativo, DBMS (Data Base Management Systems) y herramientas de desarrollo
- Sistema de comunicaciones débiles, sin protección
- Entrenamiento insuficiente el R.H.
- Ausencia de planes de sucesión o entrenamiento
- Áreas susceptibles de inundación

Estas debilidades pueden ser explotadas por las amenazas.

6.1.2 Evaluación de los riesgos de S.I. - Guía

Orientación sobre el análisis de los riesgos de seguridad de la información.

El análisis de riesgos tiene como objetivo determinar el nivel del riesgo.

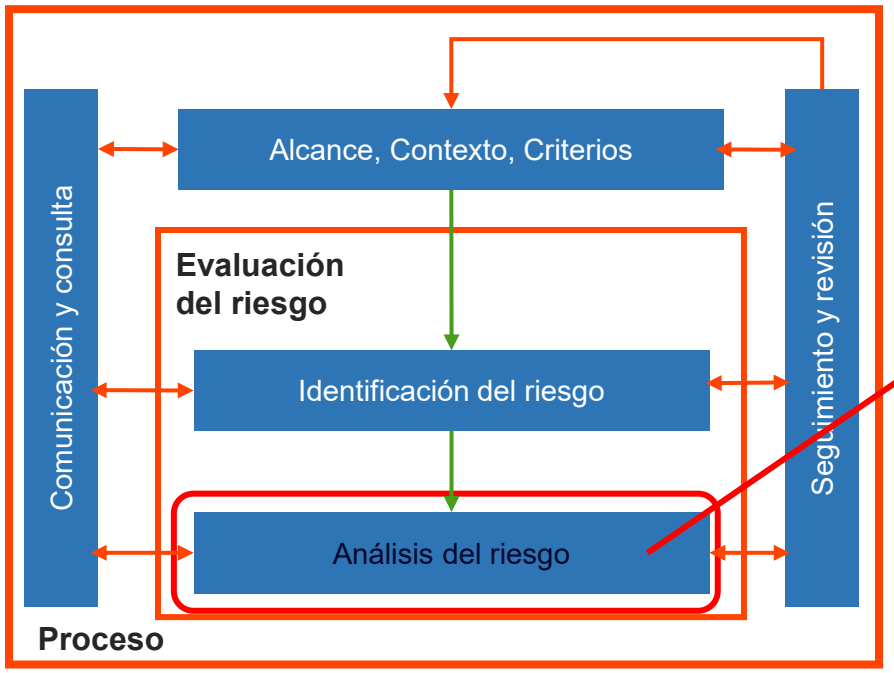
Se hace referencia a ISO 31000 en ISO IEC 27001:2022 como modelo general y requiere que para cada riesgo identificado el análisis se base en la evaluación de las **consecuencias resultantes** y **evaluar la probabilidad de que ocurran esas consecuencias para determinar un nivel de riesgo.**

Las técnicas de análisis de riesgos basadas en consecuencias y probabilidad pueden ser:
1) Cualitativo, utilizando una escala de atributos de calificación (por ejemplo, alto, medio, bajo);
2) Cuantitativo, utilizando una escala con valores numéricos (por ejemplo, costo monetario, frecuencia o probabilidad de ocurrencia); o
3) Semi-cuantitativo, utilizando escalas cualitativas con valores asignados.

Cualquiera que sea la técnica que se utilice para el análisis de riesgos, se debe considerar su nivel de objetividad.

Existen varios métodos para analizar los riesgos. Los dos enfoques mencionados (basado en eventos, en la identificación de activos, amenazas y vulnerabilidades) pueden ser adecuados para el análisis de riesgos de seguridad de la información. Los procesos de identificación y análisis de riesgos pueden ser más eficaces cuando se realicen con la ayuda de expertos en los riesgos relevantes en discusión.

6.1.2 Evaluación de los riesgos de S.I. - Metodología



El análisis del riesgo comprende las posibles consecuencias que pueden traer consigo determinadas situaciones y la probabilidad de que estas se produzcan con el objetivo de medir el nivel del riesgo.

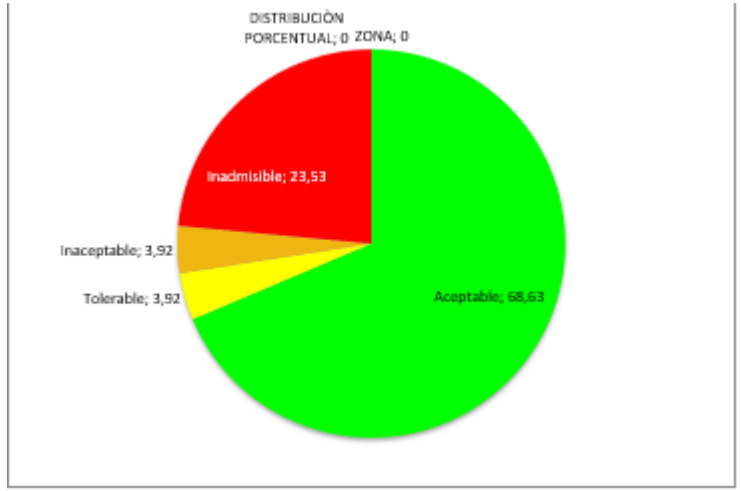
La ISO 31000 se referencia en la ISO IEC 27001 como modelo general. Para determinar un nivel de riesgo, la ISO IEC 27001 exige que para cada riesgo identificado el análisis de riesgos se basa en la valoración de las consecuencias resultantes del riesgo y en la valoración de la probabilidad de que estas consecuencias ocurran.

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Análisis del mapa riesgos

MAPA DE RIESGOS

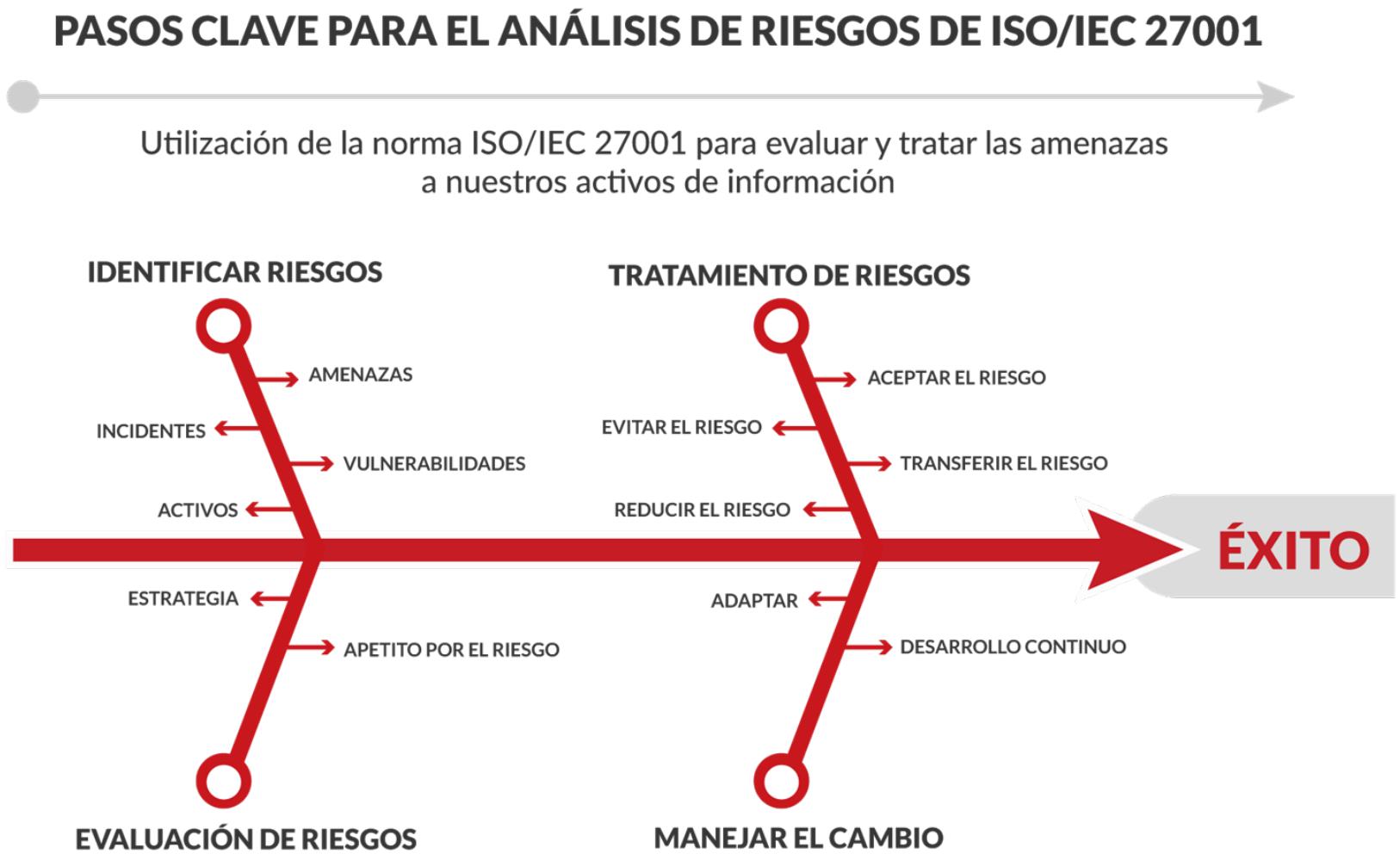
Probabilidad		Impacto				
	valor	Insignificante 1	Menor 2	Moderado 3	Mayor 4	Catastrofico 5
Casi seguro	5					
Probable	4					ATAQUES INFORMÁTICOS -- ALMACENAMIENTO || ATAQUES INFORMÁTICOS -- SERVIDOR F_E | ATAQUES INFORMÁTICOS -- CONOCIMIENTO NEGOCIO || COMPROMISO DE LA INFORMACIÓN -- CONOCIMIENTO NEGOCIO ||
Posible	3		PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL || PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO ||		COMPROMISO DE LAS FUNCIONES -- CONOCIMIENTO NEGOCIO ||	ACCIONES NO AUTORIZADAS -- CONOCIMIENTO NEGOCIO || COMPROMISO DE LA INFORMACIÓN -- DOMINA DIGITAL F_E || COMPROMISO DE LA INFORMACIÓN -- SOFTWARE GESTION F_E ||
Improbable	2	ACCIONES NO AUTORIZADAS - REDES ||	EVENTO NATURAL -- REDES || PERDIDA DE SERVICIOS ESCENCIALES -- REDES || FALLAS TECNICAS -- REDES || FALLAS TECNICAS -- SERVIDOR LOCAL || FALLAS TECNICAS -- EQUIPO DE CÓMPUTO || FALLAS TECNICAS -- EQUIPO MÓVIL || DAÑO FÍSICO -- SERVIDOR LOCAL || DAÑO FÍSICO - EQUIPO DE CÓMPUTO || DAÑO			FALLAS TECNICAS -- DOMINA DIGITAL F_E || FALLAS TECNICAS -- SOFTWARE GESTION F_E || PERSONAL NO SATISFECHO -- DOMINA DIGITAL F_E || PERSONAL NO SATISFECHO -- CONOCIMIENTO NEGOCIO ||
Raro	1	EVENTO NATURAL -- INFORM. FÍSICA 1 || EVENTO NATURAL -- INFORM. FÍSICA 2 || DAÑO	EVENTO NATURAL -- EQUIPO DE CÓMPUTO || DAÑO FÍSICO -- REDES ||			DAÑO FÍSICO -- ALMACENAMIENTO || DAÑO FÍSICO -- SERVIDOR F_E ||



Aceptable	Riesgo inferior, gestionar mediante procedimientos de rutina
Tolerable	Riesgo moderado, se debe especificar la responsabilidad de la dirección.
Inaceptable	Alto riesgo, es necesario la atención de la alta dirección
Inadmisible	Riesgo extremo, se requiere acción inmediata.

Tabla 1. Categorías riesgos

6.1.2 Evaluación de los riesgos de S.I. - Metodología



6.1.2 Evaluación de los riesgos de S.I. - Guía

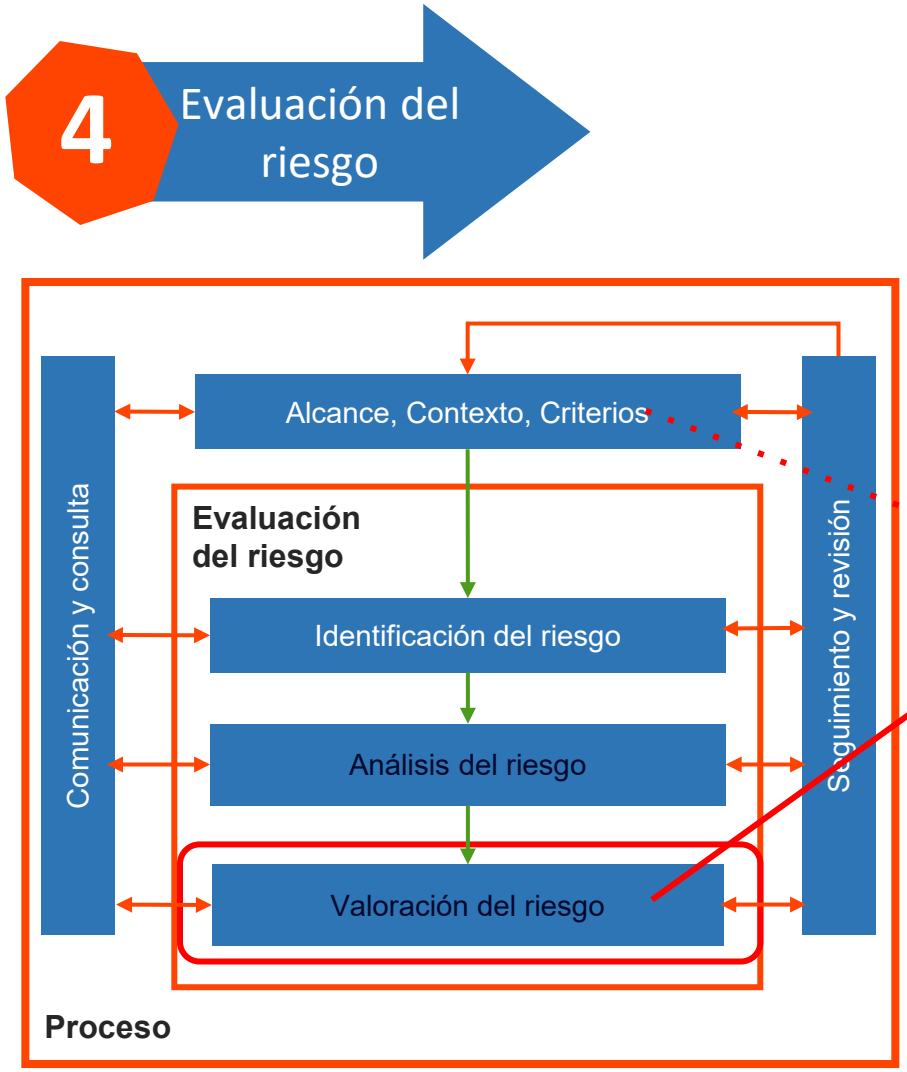
Orientación sobre la evaluación de los riesgos de seguridad de la información.

La evaluación de los riesgos analizados implica utilizar los procesos de toma de decisiones de la organización para comparar el nivel de riesgo evaluado para cada riesgo con los criterios de aceptación predeterminados para determinar las opciones de tratamiento de riesgos.

Este último paso de la evaluación de riesgos verifica si los riesgos que han sido analizados en el paso anterior pueden aceptarse de acuerdo con los criterios de aceptación definidos o necesitan más tratamiento. También proporciona información sobre la magnitud del riesgo, pero no información inmediata sobre la urgencia de implementar opciones de tratamiento de riesgos. Dependiendo de las circunstancias en las que ocurren riesgos, pueden tener diferentes prioridades de tratamiento. Por lo tanto, el resultado de este paso debería ser una lista de riesgos en orden de prioridad.

Es útil conservar más información sobre estos riesgos de los pasos de identificación y análisis de riesgos para respaldar las decisiones de tratamiento de riesgos.

6.1.2 Evaluación de los riesgos de S.I. - Metodología



La evaluación de los riesgos analizados involucra el uso de los procesos de toma de decisiones de la organización **para comparar el nivel valorado de riesgo para cada riesgo con los criterios de aceptación predeterminados**, para determinar las opciones de tratamiento de riesgos.

Este paso final de la valoración de riesgos verifica si los riesgos que han sido analizados en los pasos anteriores pueden ser aceptados de acuerdo con los criterios de aceptación definidos.

La salida de este paso debería ser una lista de riesgos en orden de prioridad.

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Probabilidades de Ocurrencias		
Calificación	**Atributo**	**Descripción**
1	Raro	Ocurrencia excepcional
2	Improbable	Difícil que ocurra
3	Posible	Normalmente NO ocurre
4	Probable	Existen razones que creer que ocurrirá
5	Frecuente	Normalmente ocurre

Potencial Impacto		
Calificación	**Atributo**	**Descripción**
1	Insignificante	Sin perjuicios
2	Menor	Es controlable
3	Moderado	Requiere intervención de terceros
4	Mayor	Pérdida de capacidad , efectos nocivos
5	Catastrófico	Imposibilidad de reacción

Matriz de Niveles de Riesgos					
Probabilidad de Ocurrencia	Impacto Potencial				
	1	2	3	4	5
1	L	L	M	H	H
2	L	L	M	H	E
3	L	M	H	E	E
4	M	H	H	E	E
5	H	H	E	E	E

Controles		
Calificación	Atributo	Descripción
1	Incontrolable	Ausencia de control con respecto a la probabilidad de ocurrencia y la posibilidad de gestionar las consecuencias
2	Débil	Controles insuficientes para prevenir o mitigar el riesgo o ***NO SE CONOCEN***
3	Moderado	Los controles ***NO*** permiten la gestión de todos los sucesos de riesgos potenciales
4	Fuerte	Los controles económicamente viables se gestionan. Se hace seguimiento y monitoreo

6.1.2 Evaluación de los riesgos de S.I. - Metodología

Lista de riesgos en orden de prioridad.

Probabilidad de ocurrencia

Impacto en las operaciones

ESCENARIO	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto
EVENTO NATURAL -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto	1	1
EVENTO NATURAL -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto	1	1
EVENTO NATURAL -- REDES	Poco probable	2	Muy bajo	2	4
EVENTO NATURAL -- EQUIPO DE CÓMPUTO	Muy poco probable	1	Muy bajo	2	2
PERDIDA DE SERVICIOS ESCENCIALES -- REDES	Poco probable	2	Muy bajo	2	4
PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL	Probable	3	Muy bajo	2	6
PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO	Probable	3	Muy bajo	2	6
FALLAS TECNICAS -- DOMINA DIGITAL F_E	Poco probable	2	Alto	5	10
FALLAS TECNICAS -- SOFTWARE GESTION F_E	Poco probable	2	Alto	5	10
FALLAS TECNICAS -- REDES	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- SERVIDOR LOCAL	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- EQUIPO DE CÓMPUTO	Poco probable	2	Muy bajo	2	4
FALLAS TECNICAS -- EQUIPO MÓVIL	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto	1	1
DAÑO FÍSICO -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto	1	1
DAÑO FÍSICO -- REDES	Muy poco probable	1	Muy bajo	2	2
DAÑO FÍSICO -- SERVIDOR LOCAL	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- EQUIPO DE CÓMPUTO	Poco probable	2	Muy bajo	2	4
DAÑO FÍSICO -- EQUIPO MÓVIL	Poco probable	2	Muy bajo	2	4

6.1.3 Tratamiento de riesgos de S.I. - Requisito

La organización define y aplica un proceso de tratamiento de riesgos de seguridad de la información.

El tratamiento de riesgos de seguridad de la información es el proceso general de selección de opciones de tratamiento de riesgos, determinar los controles apropiados para implementar dichas opciones, formular un plan de tratamiento de riesgos y obtener la aprobación del plan de tratamiento de riesgos por parte de los propietarios del riesgo.

Todos los pasos del proceso de tratamiento de riesgos de seguridad de la información, así como los resultados deben ser conservados por la organización como información documentada.

6.1.3 Tratamiento de riesgos de S.I. - Guía

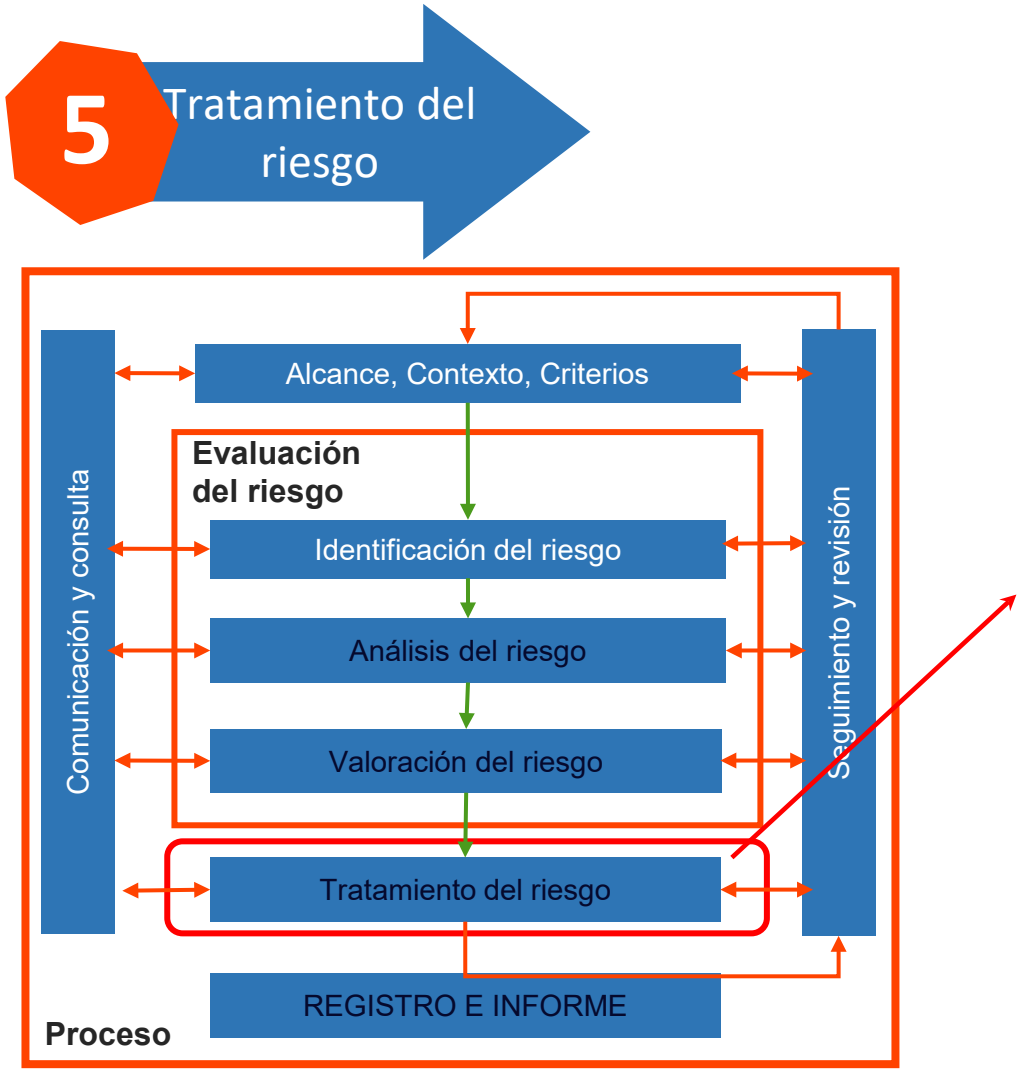
Orientación sobre opciones de tratamiento de riesgos de seguridad de la información.

Las opciones de tratamiento de riesgos son:

a) **Evitar** el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo o eliminando la fuente de riesgo (por ejemplo, cerrando un portal de comercio electrónico);
b) **Asumir** riesgos adicionales o aumentarlos para aprovechar una oportunidad de negocio (por ejemplo, abrir una portal de comercio electrónico);
c) **Modificar** el riesgo cambiando la probabilidad (por ejemplo, reduciendo las vulnerabilidades) o las consecuencias (por ejemplo, diversificar activos) o ambos;
d) **Compartir** el riesgo con otras partes mediante seguros, subcontratación o financiación de riesgos; y
e) **Retener** el riesgo basándose en los criterios de aceptación del riesgo o mediante una decisión informada (por ejemplo, mantener el portal de comercio electrónico existente tal como está).

Cada riesgo individual debe ser tratado de acuerdo con los objetivos de seguridad de la información por uno o más de estas opciones, con el fin de cumplir con los criterios de aceptación del riesgo.

6.1.3 Tratamiento de riesgos de S.I. - Metodología



El tratamiento de riesgos de seguridad de la información es el proceso global de **selección de opciones de tratamiento de riesgos**, **determinación de controles apropiados** para implementar estas opciones, **formulación de un plan de tratamiento de riesgos** y la **obtención de aprobación del plan de tratamiento de riesgos** por parte del(los) dueño(s) del(los) riesgos.

Las opciones de tratamiento de riesgos son:

- Evitar el riesgo
- Asumir el riesgo
- Modificar el riesgo
- Compartir el riesgo
- Retener el riesgo

6.1.3 Tratamiento de riesgos de S.I. - Metodología

¿Riesgo = Incertidumbre?

Es la potencialidad que una amenaza explote las vulnerabilidades de los A.I., se convierta en un desastre y afecten los objetivos de la Organización (económicas, ambientales, imagen, reputación, sociales).

Puede ser positivo o negativo.

Tratamiento del Riesgo: Es una práctica metodológica y sistemática que se ejecuta para identificar, medir, clasificar y definir las procedimientos, políticas y acciones.

6.1.3 Tratamiento de riesgos de S.I. - Guía

Orientación para determinar los controles necesarios

Se debe prestar especial atención a la determinación de los controles necesarios de seguridad de la información.

Cualquier control debe determinarse con base en los riesgos de seguridad de la información previamente evaluados.

Si una organización tiene una mala evaluación de riesgos de seguridad de la información, tiene una base pobre para su elección de controles de seguridad de la información.

Una determinación de control adecuada garantiza:

Que incluya los controles necesarios y no elija controles innecesarios; el diseño de los controles necesarios satisface una amplitud y profundidad apropiadas.

Como consecuencia de una mala elección de controles, el tratamiento de riesgos de seguridad de la información propuesto puede ser ineficaz o ineficiente y, por tanto, costosos.

6.1.3 Tratamiento de riesgos de S.I. - Guía

Por lo tanto, para garantizar que el tratamiento de los riesgos de seguridad de la información sea eficaz y eficiente, es importante **ser capaz de demostrar la relación desde los controles necesarios hasta los resultados del riesgo**.

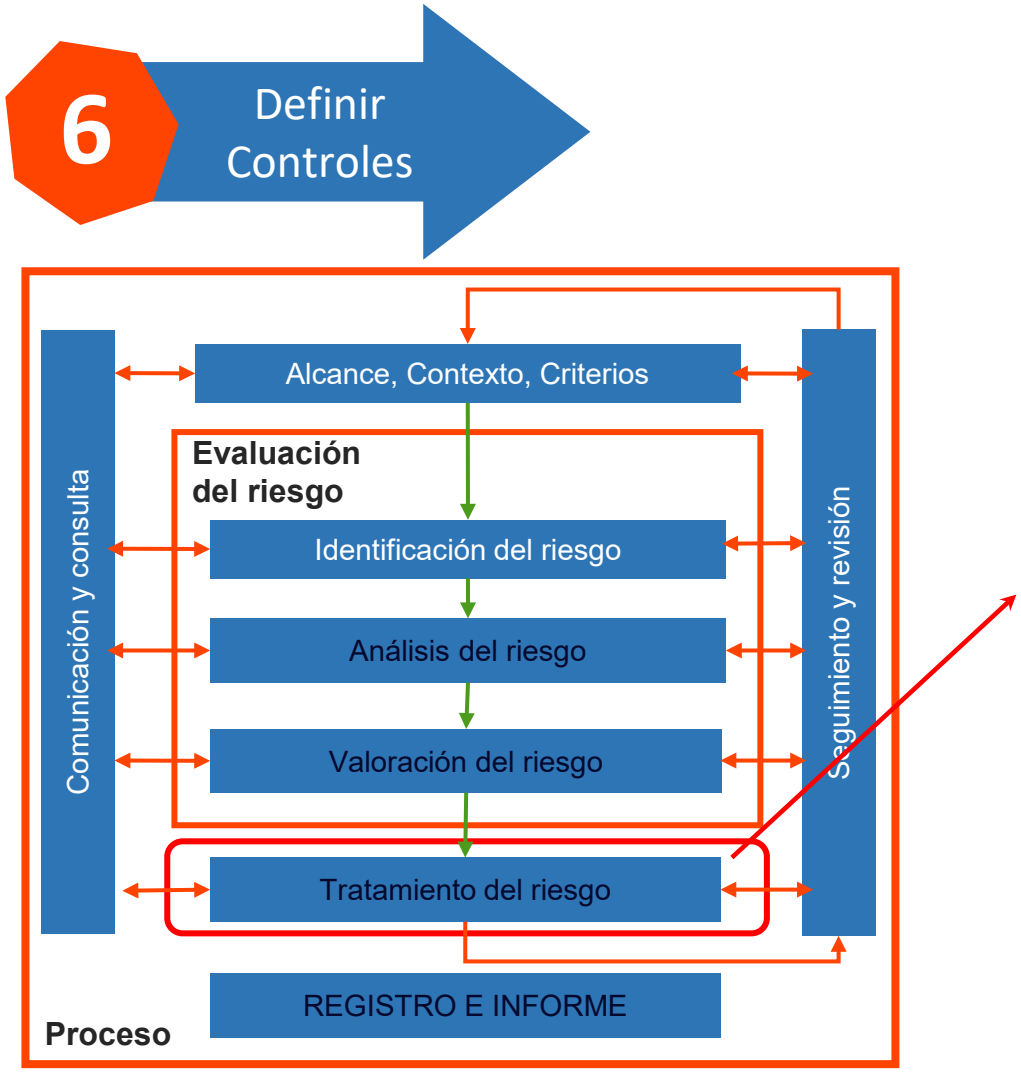
Al definir procesos de evaluación y tratamiento de riesgos puede ser necesario utilizar múltiples controles para lograr el tratamiento requerido, por ejemplo, si se elige la opción de cambiar las consecuencias de un evento en particular puede requerir controles para efectuar la detección rápida del evento, así como controles para responder y recuperarse del evento.

Al determinar los controles, la organización también debe tener en cuenta los controles necesarios para servicios de proveedores externos de aplicaciones, procesos y funciones. Normalmente, estos controles están obligados a introducir requisitos de seguridad de la información en los acuerdos con estos proveedores, incluyendo formas de obtener información sobre en qué medida se cumplen estos requisitos.

Puede haber situaciones en las que la organización desee determinar y describir controles detallados siendo parte de su propio SGSI aunque los controles sean realizados por proveedores externos.

Independientemente del enfoque adoptado, la organización siempre debe considerar los controles necesarios en sus proveedores para su SGSI.

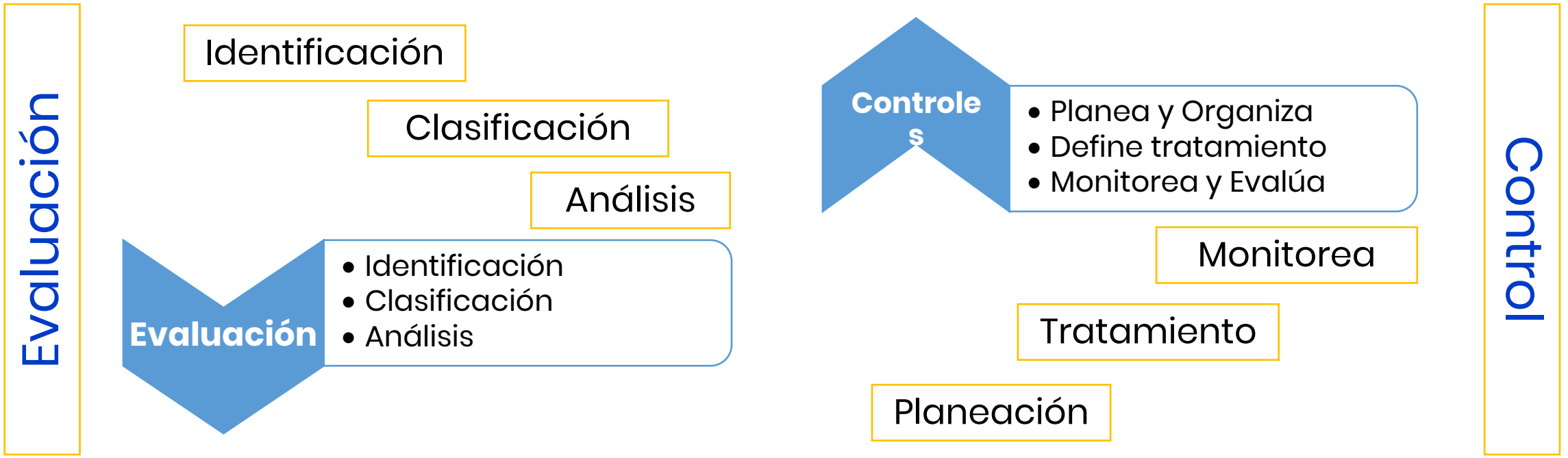
6.1.3 Tratamiento de riesgos de S.I. - Metodología



Para asegurar que el tratamiento de riesgos de seguridad de la información sea eficaz y eficiente, es importante estar en capacidad de demostrar la relación entre los controles necesarios y los resultados de los procesos de valoración y tratamiento de riesgos.

Puede ser necesario usar múltiples controles para lograr el tratamiento requerido del riesgo de seguridad de la información. Por ejemplo, si se escoge la opción de cambiar las consecuencias de un evento particular, se pueden requerir controles para detectar con prontitud el evento y controles para responder y recuperarse del evento.

6.1.3 Tratamiento de riesgos de S.I. - Metodología



6.1.3 Tratamiento de riesgos de S.I. - Guía

Orientación sobre la comparación de controles con los de ISO IEC 27001:2022, Anexo A

ISO/IEC 27001:2022, Anexo A contiene una lista completa de objetivos y controles de control.

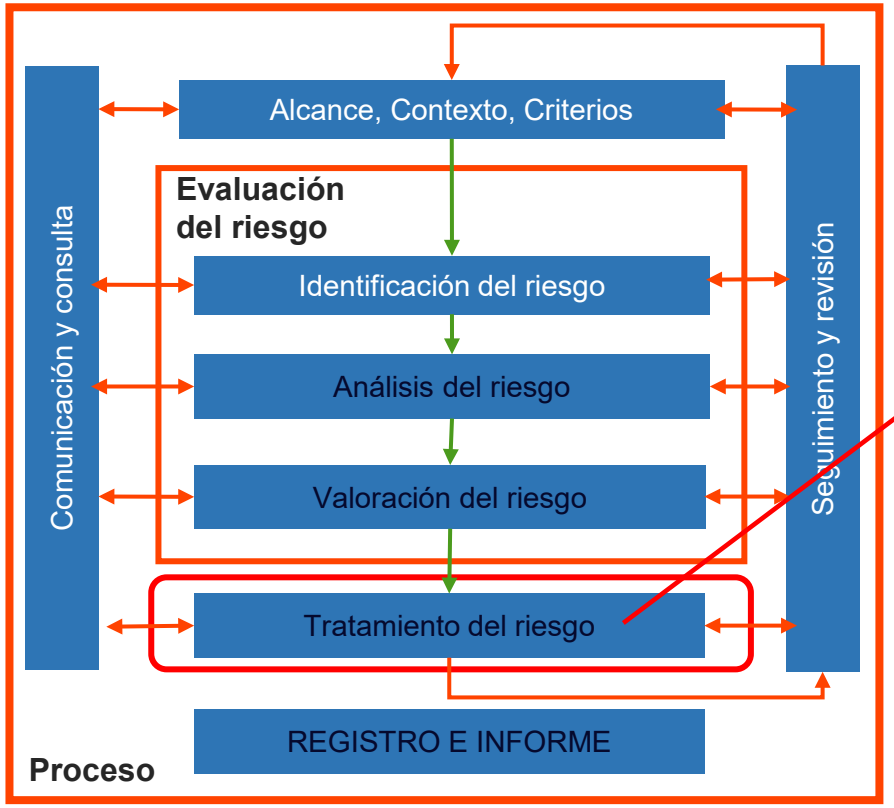
Líderes implementadores de ISO IEC 27001:2022 deben garantizar que no se pasen por alto ningún control necesario comparándolos con ISO/IEC 27001:2022, Anexo A

También puede identificar controles alternativos que pueden ser más efectivos en modificar el riesgo de seguridad de la información.

Los controles enumerados en la ISO IEC 27001:2022 Anexo A no son exhaustivos y los objetivos y controles de control adicionales deben agregarse según sea necesario.

No es necesario incluir todos los controles dentro de ISO IEC 27001:2022, Anexo A, **no obstante, cualquier control dentro de ISO/IEC 27001:2022, Anexo A que no contribuya a modificar el riesgo puede excluirse pero debe justificarse la exclusión.**

6.1.3 Tratamiento de riesgos de S.I. - Metodología



La organización debe garantizar que no se pasen por alto ningún control necesario comparándolos con ISO/IEC 27001:2022, Anexo A

6.1.3 Tratamiento de riesgos de S.I. - Guía

Orientación sobre la elaboración de una Declaración de Aplicabilidad

El SoA contiene:
— todos los controles **considerados como necesarios para la organización** y, para cada control:
— la justificación de la inclusión del control; y
— si el control está implementado, completamente implementado, en progreso, o aún no comienza; y
— la justificación para excluir cualquiera de los controles de la norma ISO IEC 27001: 2022, anexo A.

La justificación para incluir un control se basa en parte en el efecto del control al modificar una información de riesgo de seguridad.

Una referencia a los resultados de la evaluación de riesgos de seguridad de la información y la seguridad de la información.

El plan de tratamiento de riesgos debe ser suficiente, junto con la modificación del riesgo de seguridad de la información esperada mediante la aplicación de los controles necesarios.

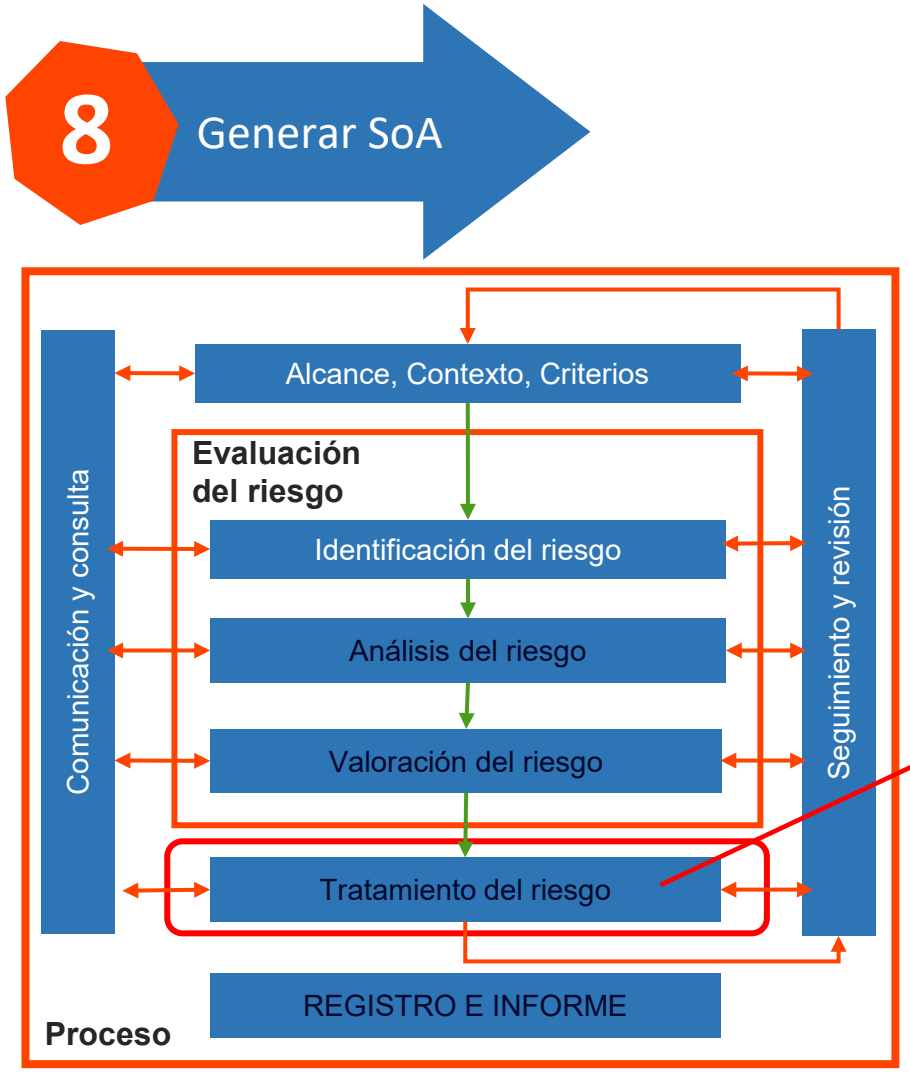
6.1.3 Tratamiento de riesgos de S.I. - Guía

La justificación para excluir un control contenido en ISO/IEC 27001:2022, Anexo A puede incluir lo siguiente:
— se ha determinado que el control no es necesario para implementarse.
— el control no es aplicable porque está fuera del alcance del SGSI.
— se evita mediante un control personalizado.

NOTA:
Un control personalizado es un control no incluido en ISO/IEC 27001:2022, Anexo A.
Se puede producir un SoA útil como una tabla que contiene los 93 controles de la ISO IEC 27001:2022, Anexo A con los controles adicionales que no se mencionan en la ISO IEC 27001:2022.

Una columna de la tabla puede indicar si es necesario implementar un control o no e incluir las opciones de tratamiento de riesgo, una siguiente columna puede contener la justificación de la inclusión o exclusión, y una última columna de la tabla puede indicar el estado actual de implementación del control. Se pueden utilizar columnas adicionales, para detalles no requeridos por ISO IEC de cómo se realiza el control implementado o una referencia cruzada a una descripción más detallada e información documentada o políticas relevantes para implementar el control o responsabilidades para la operación de cada control.

6.1.3 Tratamiento de riesgos de S.I. - Metodología



La comparación de los controles con los de ISO IEC 27001:2022, Anexo A del paso anterior debe realizarse contra la declaración de aplicabilidad (SoA) ya que este contiene todos los controles c**onsiderados como necesarios para la organización**, si el control está implementado o no y la justificación de la inclusión o exclusión.

6.1.3 Tratamiento de riesgos de S.I. - Metodología

Declaración de Aplicabilidad (Statement of Applicability –SoA)

CONTROL DE REFERENCIA	NOMBRE DEL CONTROL	DESCRIPCIÓN DEL CONTROL	APLICABLE SÍ/NO	RAZÓN DE SELECCIÓN DE CONTROL	JUSTIFICACIÓN DE EXCLUSIÓN DEL CONTROL
A.6.2.2	Teletrabajo	Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo	NO		No se realiza teletrabajo dentro de la organización
A.18.1.2	Derechos de propiedad intelectual	Deben implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados	SÍ	Se cumple con las normativas sobre derechos de propiedad intelectual	

6.1.3 Tratamiento de riesgos de S.I. - Guía

Orientación sobre la formulación de un plan de tratamiento de riesgos de seguridad de la información.

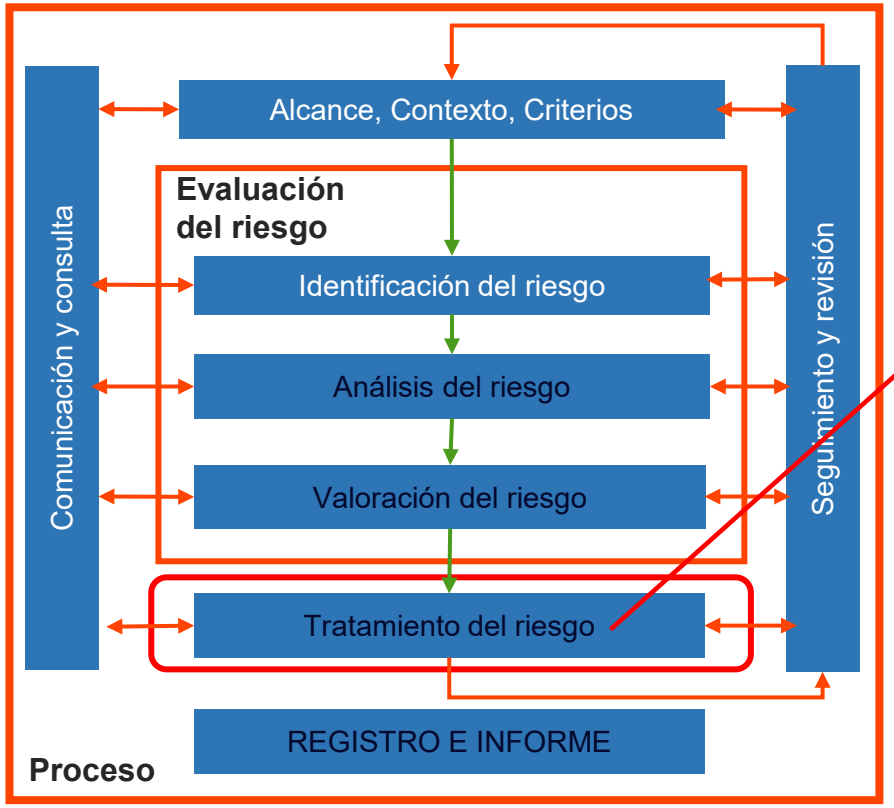
La norma ISO IEC 27001 no especifica una estructura o contenido para el plan tratamiento de riesgos de seguridad de la información.

Sin embargo, el plan debe formularse a partir de los resultados del paso anterior. Por lo tanto, el plan debe documentar para cada riesgo tratado:
— opciones de tratamiento seleccionadas;
— controles necesarios; y
— estado de implementación.

Otro contenido útil puede incluir:
— propietario(s) del riesgo; y
— riesgo residual esperado tras la ejecución de las acciones.

Si el plan de tratamiento de riesgos requiere alguna acción, entonces se debe planificar indicando responsabilidades y plazos.

6.1.3 Tratamiento de riesgos de S.I. - Metodología



Diseñar un plan de tratamiento de riesgo.

6.1.3 Tratamiento de riesgos de S.I. - Metodología

Plan de tratamiento de riesgos.

CÓDIGO RIESGO	DESCRIPCIÓN	NIVEL DE RIESGO	PROCESO DE NEGOCIO	ACTIVOS RELACIONADOS	ESTRATEGIA	ACCIONES A DESARROLLAR	CONTROL DE REFERENCIA ANEXO A	TIPO DE CONTROL	RESPONSABLE	PLAZO

6.1.3 Tratamiento de riesgos de S.I. - Guía

Orientación sobre cómo obtener la aprobación de los propietarios de riesgos

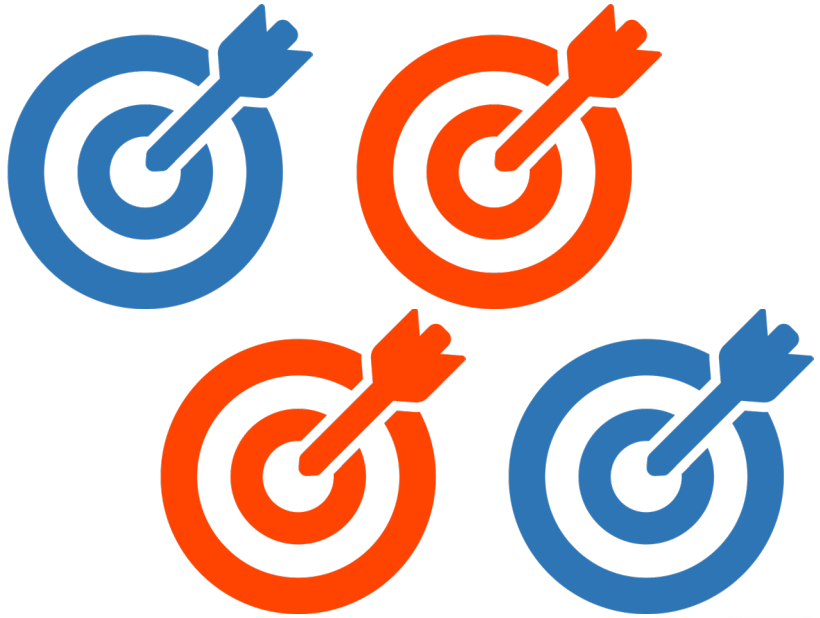
Cuando se formula el plan de tratamiento de riesgos de seguridad de la información, la organización debe obtener la autorización de los **propietarios del riesgo**. Dicha autorización debe basarse en una aceptación de riesgo definida, criterios o concesión justificada si se desvían de ellos.

A través de sus procesos de gestión, la organización debe **registrar la aceptación del riesgo** por parte del propietario del riesgo residual y aprobación por la dirección del plan.

Por ejemplo, la aprobación del propietario de este riesgo se puede documentar modificando el plan de tratamiento de riesgos por columnas que indican la efectividad del control, el valor residual riesgo y la aprobación del propietario del riesgo.

6.2 Objetivos de Seguridad de la Información – Requisito

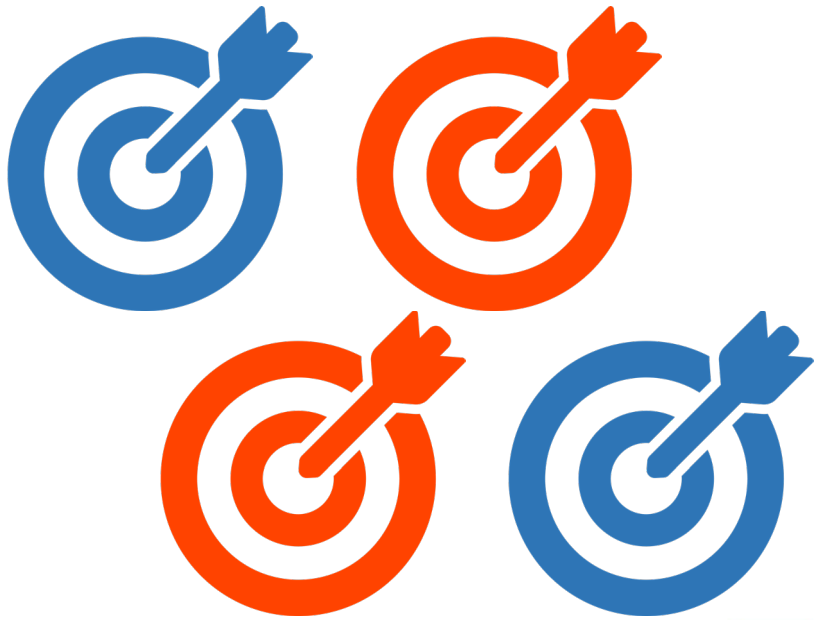
La organización establece objetivos de seguridad de la información y planea cómo alcanzarlos en los niveles y funciones relevantes.



6.2 Objetivos de Seguridad de la Información – Explicación

Los objetivos de seguridad de la información ayudan a implementar las metas estratégicas de una organización, así
como a implementar la política de seguridad de la información. Por tanto, los objetivos de un SGSI son la seguridad de la información, objetivos de confidencialidad, integridad y disponibilidad de la información.

Los objetivos de seguridad de la información también ayudan a especificar y medir el desempeño de los controles y procesos de seguridad de la información de acuerdo con la política de seguridad de la información.



La organización planifica, establece y emite objetivos de seguridad de la información para las funciones y niveles relevantes.

Los requisitos de la norma ISO/EC 27001 relativos a los objetivos de seguridad de la información se aplican a todos los objetivos de seguridad.

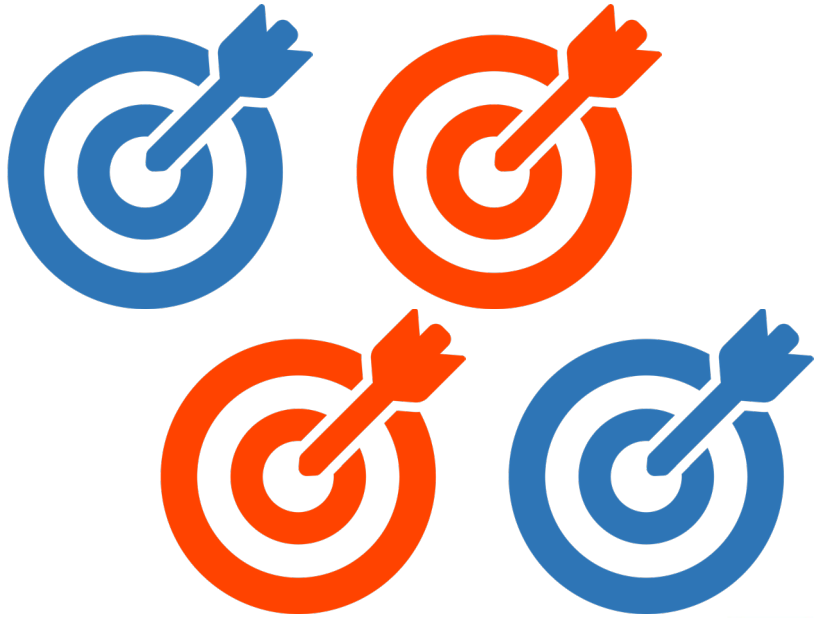
6.2 Objetivos de Seguridad de la Información – Explicación

Si la política de seguridad de la información contiene objetivos, entonces esos objetivos son requeridos para cumplir con los criterios en 6.2.

Si la política contiene un marco para establecer objetivos, entonces los objetivos producidos por ese marco deben cumplir con los requisitos de 6.2.

Los requisitos a tener en cuenta a la hora de establecer objetivos son los que se determinan al comprender la organización y su contexto (ver 4.1), así como las necesidades y expectativas de partes interesadas (ver 4.2).

Los resultados de las evaluaciones de riesgos y los tratamientos de riesgos se utilizan como insumo para la revisión continua de los objetivos para asegurar que sigan siendo apropiados a las circunstancias de una organización. Los objetivos de seguridad de la información son insumos para la evaluación de riesgos: criterios y criterios de aceptación de riesgos y para realizar evaluaciones de riesgos de seguridad de la información



6.2 Objetivos de Seguridad de la Información – Explicación

Los objetivos de seguridad de la información deben:

1. Ser coherentes con la política de seguridad de la información.
2. Ser medibles, si es posible; esto significa que es importante estar en capacidad de determinar si se ha cumplido o no un objetivo.
3. Estar vinculados a los requisitos de seguridad de la información aplicables y a los resultados de la valoración y tratamiento de riesgos.
4. Ser comunicados.
5. Ser actualizados, según sea apropiado.

6.2 Objetivos de Seguridad de la Información – Explicación

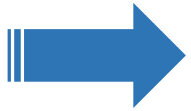
Al planificar cómo lograr sus objetivos de seguridad de la información, la organización determina:

- Qué se hará.
- Qué recursos son necesarios
- Quién se hará responsable
- Cuándo se completa
- Cómo se evaluarán los resultados

6.2 Objetivos de Seguridad de la Información – Guía

La política de seguridad de la información debe establecer los objetivos de seguridad de la información o proporcionar un marco para fijar los objetivos.

Los objetivos de seguridad de la información se pueden expresar de diversas maneras



- Valores numéricos con sus límites, por ejemplo, "no sobrepase un nivel determinado", y "alcance el nivel 4".
- Las metas para las mediciones del desempeño de seguridad de la información.
- Las metas para las mediciones de la eficacia del SGSI.
- El cumplimiento con ISO IEC 27001; – el cumplimiento con los procedimientos del SGSI.
- La necesidad de finalizar acciones y planes; y
- Los criterios de riesgo por cumplir.

6.2 Objetivos de Seguridad de la Información – Guía

Guía para cada requisito

1 Ser coherentes con la política de seguridad de la información.

La política de seguridad de la información especifica los requisitos para la seguridad de la información en una organización.

Todos los demás requisitos específicos establecidos para funciones y niveles relevantes deben ser consistente con ellos.

Si la política de seguridad de la información tiene objetivos de seguridad de la información, entonces cualquier otro objetivo específico de seguridad de la información debe estar vinculado a los de la información política de seguridad.

Si la política de seguridad de la información sólo proporciona el marco para establecer objetivos, entonces se debe seguir ese marco y garantizar que se vinculen objetivos más específicos a los más genéricos.

6.2 Objetivos de Seguridad de la Información- Guía

Guía para cada requisito

2 Ser medibles, si es posible; esto significa que es importante estar en capacidad de determinar si se ha cumplido o no un objetivo.

No todos los objetivos pueden ser medibles, pero hacer que los objetivos sean medibles apoya a los logros y mejora.

Es muy deseable poder describir, cualitativa o cuantitativamente, el grado en que se ha cumplido un objetivo.

Por ejemplo, para orientar las prioridades de esfuerzo adicional si no se cumplen los objetivos, o para proporcionar información sobre oportunidades para mejorar la efectividad si se superan los objetivos.

Debería ser posible entender si se ha logrado o no, cómo se determina el logro de los objetivos y si es posible lograrlos mediante medidas.

6.2 Objetivos de Seguridad de la Información – Guía

Guía para cada requisito

3 Estar vinculados a los requisitos de seguridad de la información aplicables y a los resultados de la valoración y tratamiento de riesgos.

Los objetivos de seguridad de la información deben estar alineados con las necesidades de seguridad de la información;

Por esta razón, **la evaluación de riesgos y los resultados del tratamiento** deben usarse como insumos al establecer objetivos de seguridad de la información.

6.2 Objetivos de Seguridad de la Información – Guía

Guía para cada requisito

4 Ser comunicados.

Los objetivos de seguridad de la información deben comunicarse a los interesados internos relevantes y otras partes de la organización.

También podrán comunicarse a partes interesadas externas, como clientes, en la medida en que necesiten conocer y se vean afectados por la información y los objetivos de seguridad.

6.2 Objetivos de Seguridad de la Información – Guía

Guía para cada requisito

5 Ser actualizados, según sea apropiado.

Cuando las necesidades de seguridad de la información cambian con el tiempo, la seguridad de la información relacionada los objetivos deben actualizarse en consecuencia.

Su actualización deberá comunicarse según lo requerido en el punto anterior a las partes interesadas internas y externas según corresponda.

6.2 Objetivos de Seguridad de la Información – Guía

La organización debe planificar cómo lograr sus objetivos de seguridad de la información.

La organización podrá utilizar cualquier metodología o mecanismo que elija para planificar el logro de sus objetivos de seguridad de la información.

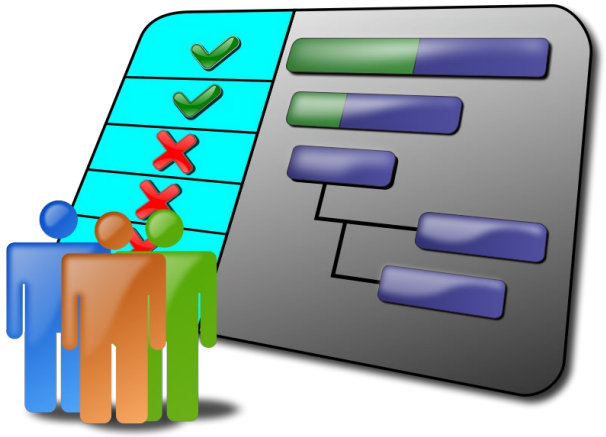
Puede haber un único plan de seguridad de la información, uno o más planes de proyecto o acciones incluidos en otros planes organizativos. Cualquiera que sea la forma que adopte la planificación, los planes resultantes deben definir como mínimo:

— las actividades a realizar;
— los recursos necesarios que deben comprometerse para ejecutar las actividades;
— las responsabilidades;
— los cronogramas y los hitos de las actividades; y
— los métodos mediciones y calendario para evaluar si los resultados alcanzan los objetivos.

La norma ISO/IEC 27001:2022 requiere que las organizaciones conserven información documentada sobre los objetivos de la seguridad de la información.

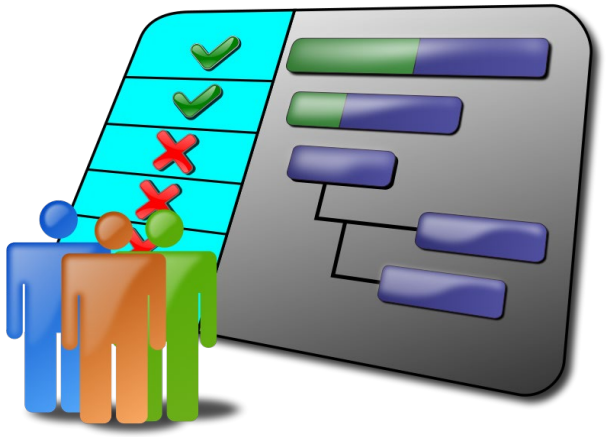
6.3 Planificación de Cambios – Requisito

Cuando la organización determina la necesidad de cambios en la gestión de seguridad de la información, estos se llevarán a cabo de forma planificada.



6.3 Planificación de Cambios – Explicación

Hay que planificar los cambios del sistema de gestión y que estos se realicen de manera controlada, existiendo un plan de cómo estos se van a implementar y validar.

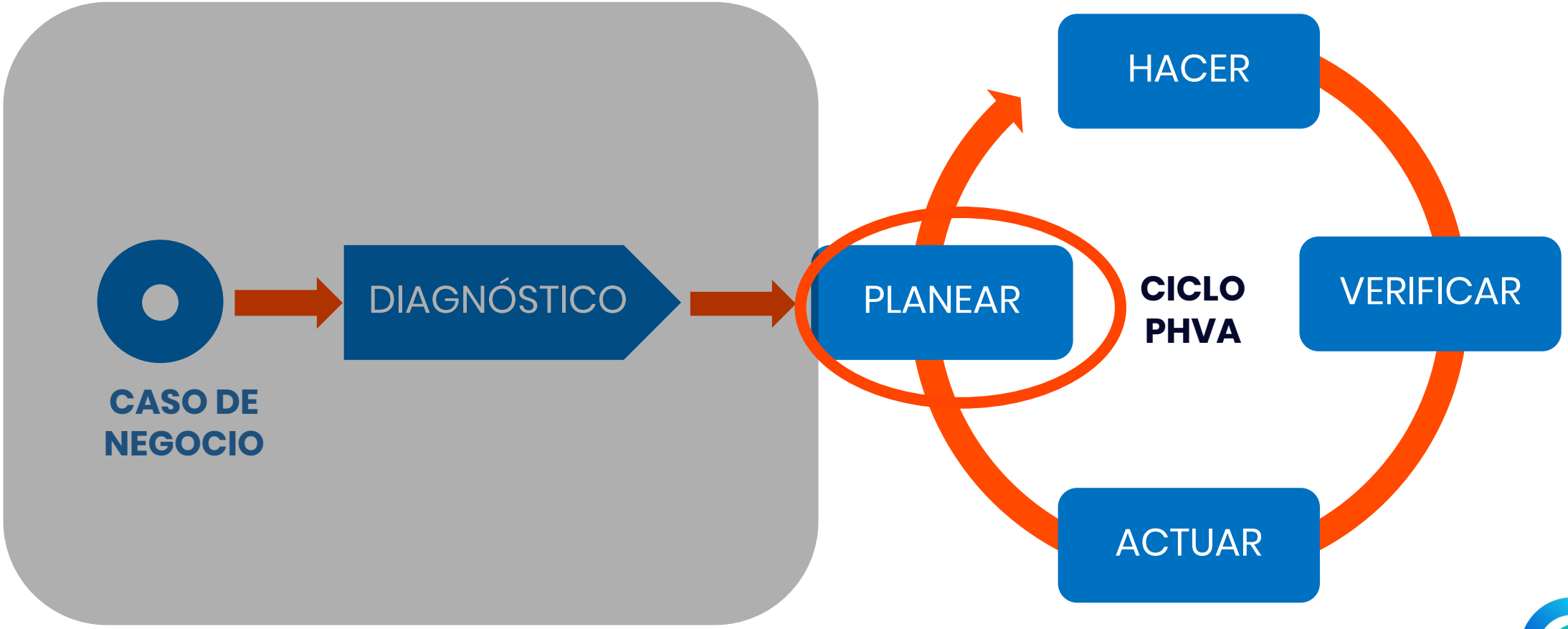


7. Soporte:
Interpretar los Requisitos de ISO IEC 27001

7.1 Recursos.
7.2 Competencia.
7.3 Toma de Conciencia.
7.4 Comunicación.
7.5 Información Documentada.
7.5.2 Creación y actualización.
7.5.3 Control.

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (Planear) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en la capacidad de crear un programa de entrenamiento y concienciación que contribuya con la efectividad del ISMS.

Estructura de ISO IEC 27001

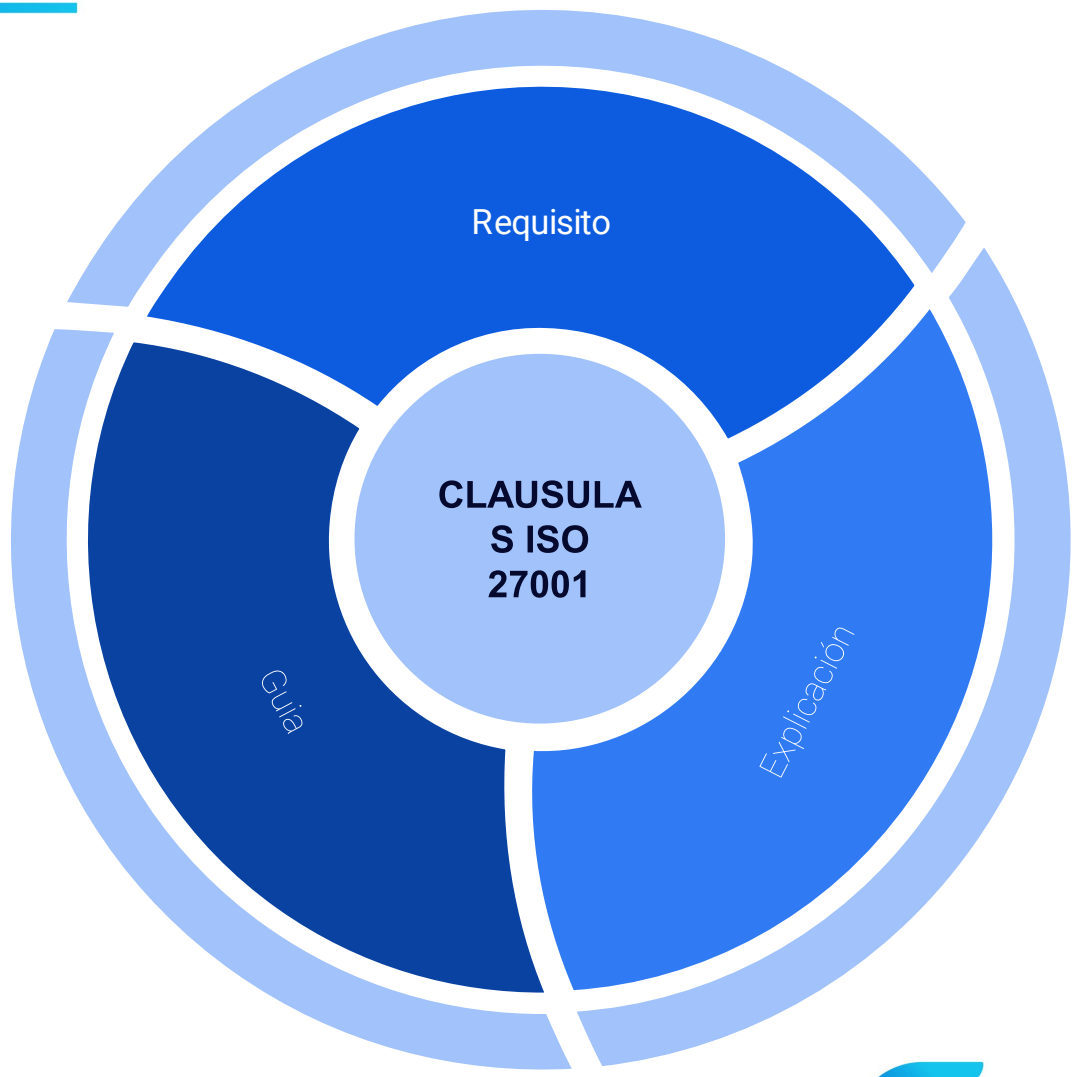
Requisitos y cómo abordarlos

En este módulo se abordan los requisitos declarados en la cláusula 7 de la ISO IEC 27001:2022 desde 3 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 7 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.



7.1 Recursos – Requisito

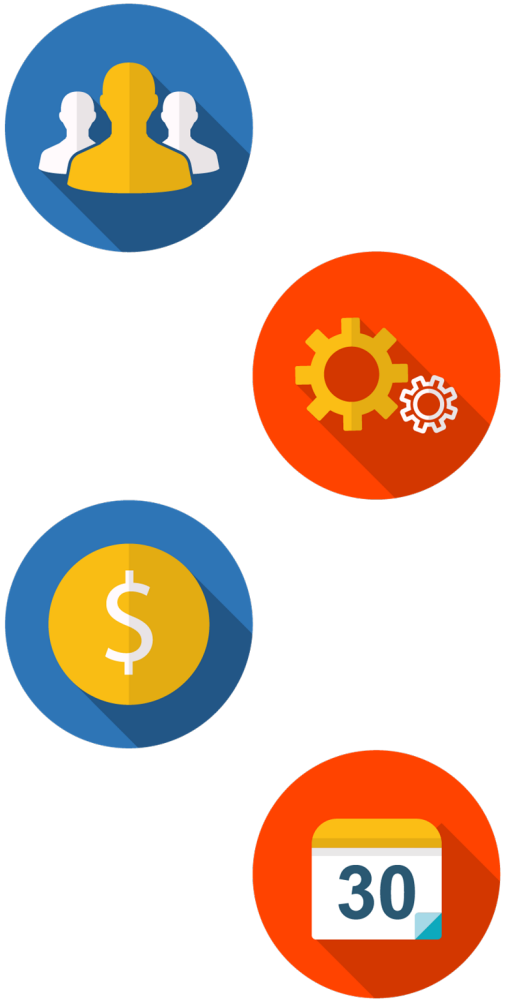
La organización determina y proporciona los recursos para establecer, implementar, mantener y mejorar continuamente el SGSI.

7.1 Recursos – Explicación

Los recursos son fundamentales para llevar a cabo cualquier tipo de actividad. Las categorías de recursos pueden incluir:

- **Personas** para conducir y operar las actividades;
- **Tiempo** para realizar las actividades y tiempo para permitir que los resultados se asienten antes de dar un nuevo paso;
- **Recursos financieros** para adquirir, desarrollar e implementar lo necesario.
- **Información** para respaldar decisiones, medir el desempeño de acciones y mejorar el conocimiento;
- **Infraestructura** y otros medios que puedan adquirirse o construirse, como tecnología, herramientas y materiales, independientemente de que sean productos de tecnologías de la información o no.

Estos recursos deben mantenerse alineados con las necesidades del SGSI y, por lo tanto, deben adaptarse cuando sea requerido.



7.1 Recursos – Guía

La organización debería:

- Estimar los recursos necesarios para todas las actividades relacionadas con el SGSI en términos de cantidad y calidad (potencial y capacidad).
- Adquirir los recursos necesarios.
- Suministrar los recursos.
- Mantener los recursos a través de los procesos y actividades específicas de todo el SGSI.
- Examinar los recursos suministrados contra las necesidades del SGSI y ajustarlos según se requiera.

La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y en la medida que la organización considere necesaria para la eficacia de su sistema de gestión.

7.1 Recursos – Guía

Es la capacidad de aplicar conocimiento y habilidades para el logro de los resultados previstos, y está influenciada por el conocimiento, la experiencia y la sabiduría.

- La competencia se relaciona con las personas que trabajan bajo el control de la organización. Esto significa que la competencia se debería gestionar para los empleados de la organización y para otras personas, según sea necesario.
- La adquisición de competencias y habilidades se puede lograr tanto interna como externamente a través de experiencia, capacitación, tutoría o contratación de personas externas.
- Para competencias que sólo se necesitan temporalmente las organizaciones pueden contratar recursos externos, cuya competencia deberá ser descrita y verificada.

7.2 Competencia - Guía

La organización debería:

- Determinar la competencia esperada para cada rol dentro del SGSI.
- Asignar los roles dentro del SGSI a las personas con la competencia requerida mediante:
  - La identificación de las personas dentro de la organización, que tengan la competencia.
  - Planificar e implementar acciones para que las personas dentro de la organización obtengan la competencia.
  - Contratar nuevas personas que tengan la competencia.
- Evaluar la eficacia de las acciones.
- Verificar que las personas sean competentes para sus roles.
- Asegurar que la competencia evolucione con el tiempo de acuerdo con las necesidades y que cumpla las expectativas.

7.2 Competencia - Guía

Se requiere información documentada adecuada como prueba de competencia.

La organización debería por lo tanto conservar la documentación sobre la competencia necesaria que afecta la seguridad de la información el desempeño y cómo esta competencia es alcanzada por las personas relevantes.

7.3 Toma de Conciencia - Requisito

Las personas que realizan trabajos bajo el control de la organización son conscientes de las medidas de seguridad de la información, políticas, su contribución a la eficacia del SGSI, beneficios de una mayor seguridad de la información e implicaciones de no ajustarse a los requisitos del SGSI.

7.3 Toma de Conciencia - Requisito

El conocimiento de las personas que trabajan bajo el control de la organización se refiere a tener los conocimientos necesarios, comprensión y motivación sobre lo que se espera de ellos en materia de seguridad de la información.

La conciencia concierne a las personas que deben conocer, comprender, aceptar y:
a) apoyar los objetivos establecidos en la política de seguridad de la información; y
b) seguir las normas para realizar correctamente sus tareas diarias en apoyo a la seguridad de la información.

7.3 Toma de Conciencia - Requisito

Además, las personas que realizan trabajos bajo el control de la organización también necesitan conocer, comprender y aceptar las implicaciones de no cumplir con los requisitos del SGSI.

Las implicaciones y consecuencias para la seguridad de la información o repercusiones para la persona.

Estas personas deben ser conscientes de que existe una política de seguridad de la información y dónde encontrar información.

Gran parte del personal de una organización no necesita conocer el contenido detallado de la política, pero si deben conocer, comprender, aceptar e implementar los objetivos de seguridad de la información y requisitos derivados de la política que afectan a su rol laboral.

Estos requisitos pueden incluirse en las normas o procedimientos que se espera que sigan para realizar su trabajo.

7.3 Toma de Conciencia -Guía

La organización debería:

- Elaborar un programa con mensajes específicos enfocados hacia cada audiencia (por ejemplo, personas internas y externas).
- Incluir necesidades y expectativas de seguridad de la información dentro de los materiales de toma de conciencia y formación sobre otros temas, para poner las necesidades de seguridad de la información en contextos operacionales pertinentes.
- Verificar el conocimiento y la comprensión de los mensajes al finalizar una sesión de toma de conciencia y aleatoriamente entre sesiones.
- Verificar si las personas actúan de acuerdo con los mensajes transmitidos y usan ejemplos de comportamiento "bueno" y "malo" para reforzar el mensaje.

7.4 Comunicación - Requisito

La organización determina las necesidades de comunicaciones internas y externas relacionadas con el SGSI.

7.4 Comunicación - Explicación

La comunicación es un proceso clave dentro de un SGSI

- La comunicación puede ser entre las partes interesadas internas a todos los niveles de la organización o entre la organización y las partes externas interesadas. La comunicación se puede iniciar dentro de la organización o por una parte externa interesada

- La organización necesita determinar:

— **qué contenidos deben comunicarse,** como políticas de seguridad de la información, objetivos, procedimientos, sus cambios, conocimiento sobre riesgos de seguridad de la información, requisitos a proveedores y retroalimentación sobre el desempeño de la seguridad de la información;

— **el momento preferido u óptimo para las actividades de comunicación;**

— **quién participará en las actividades de comunicación** y cuál es el **público objetivo** de cada esfuerzo de comunicación;

— **quién debe iniciar las actividades de comunicación**, un contenido específico puede requerir que la comunicación sea iniciada por una persona u organización específica; y

— **qué procesos** están **impulsando o iniciando** actividades de comunicación, y qué procesos están **afectados** por las actividades de comunicación.

7.4 Comunicación - Guía

La organización debería:

- Determinar qué contenido es necesario comunicar. Por ejemplo:

a) planes y resultados de la gestión de riesgos a las partes interesadas según sea necesario y apropiado, en la identificación, análisis, evaluación y tratamiento de los riesgos;
b) objetivos de seguridad de la información;
c) objetivos de seguridad de la información alcanzados, incluidos aquellos que pueden respaldar su posición en el mercado (por ejemplo, certificado ISO/IEC 27001 otorgado; alegando conformidad con datos personales leyes de protección);
d) incidentes o crisis, donde la transparencia suele ser clave para preservar y aumentar la confianza en la capacidad de la organización para gestionar la seguridad de su información y hacer frente a situaciones inesperadas.
e) roles, responsabilidades y autoridad;
f) información intercambiada entre funciones y roles según lo requieran los procesos del SGSI;
g) cambios al SGSI;
h) otros asuntos identificados mediante la revisión de los controles y procesos dentro del alcance del SGSI;

7.4 Comunicación - Guía

i) asuntos (por ejemplo, notificación de incidentes o crisis) que requieren comunicación a los organismos reguladores u otras partes interesadas; y
j) solicitudes u otras comunicaciones de partes externas como clientes, clientes potenciales, usuarios de servicios y autoridades.

La organización debe identificar los requisitos de comunicación sobre temas relevantes:
k) **quién puede comunicarse externa e internamente** (por ejemplo, en casos especiales como una violación de datos), asignar funciones específicas con la autoridad adecuada. Por ejemplo, comunicación oficial.
l) los desencadenantes o la **frecuencia de la comunicación**;
m) el **contenido** de los mensajes para las partes interesadas clave (por ejemplo, clientes, reguladores, público en general, usuarios internos importantes) basados en escenarios de impacto de alto nivel. La comunicación puede ser más eficaz si se basa en mensajes preparados y aprobados previamente por un nivel adecuado de gestión como parte de un plan de comunicación, el plan de respuesta a incidentes o el plan de continuidad del negocio.

7.4 Comunicación - Guía

n) **los destinatarios previstos de la comunicación**; En algunos casos, se debe mantener una lista (por ejemplo, para comunicar cambios en los servicios o crisis);
o) los medios y canales de comunicación. La comunicación debe utilizar medios y canales específicos, para asegurarse de que el mensaje sea oficial y tenga la autoridad adecuada.
Los canales deben abordar cualquier necesidad de **protección de la confidencialidad e integridad** de la información transmitida; y
p) el proceso diseñado y el método para garantizar que los mensajes se envíen y se hayan recibido correctamente y entendido.

La comunicación debe clasificarse y manejarse de acuerdo con los requisitos de la organización.

La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y a la medida que la organización considere necesaria para la eficacia de su sistema de gestión.

7.5.1 Información Documentada - Requisito

La organización incluye información documentada en el SGSI según lo exige directamente la norma ISO IEC 27001:2022, así como la determinada por la organización como necesaria para la efectividad del SGSI.

7.5.1 Información Documentada – Explicación

Es necesaria para:

- Definir y comunicar los objetivos, la política, directrices, instrucciones, controles, procesos, procedimientos de seguridad de la información y qué personas o grupos de personas se espera que lo hagan, y cómo se espera que lo lleven a cabo.
- Las auditorías del SGSI y para mantener un SGSI estable cuando se cambian las personas que están en los roles clave.
- Para registrar las acciones, decisiones y resultados de los procesos de SGSI y los controles de seguridad de la información.

7.5.1 Información Documentada - Explicación

Estructura típica de la documentación

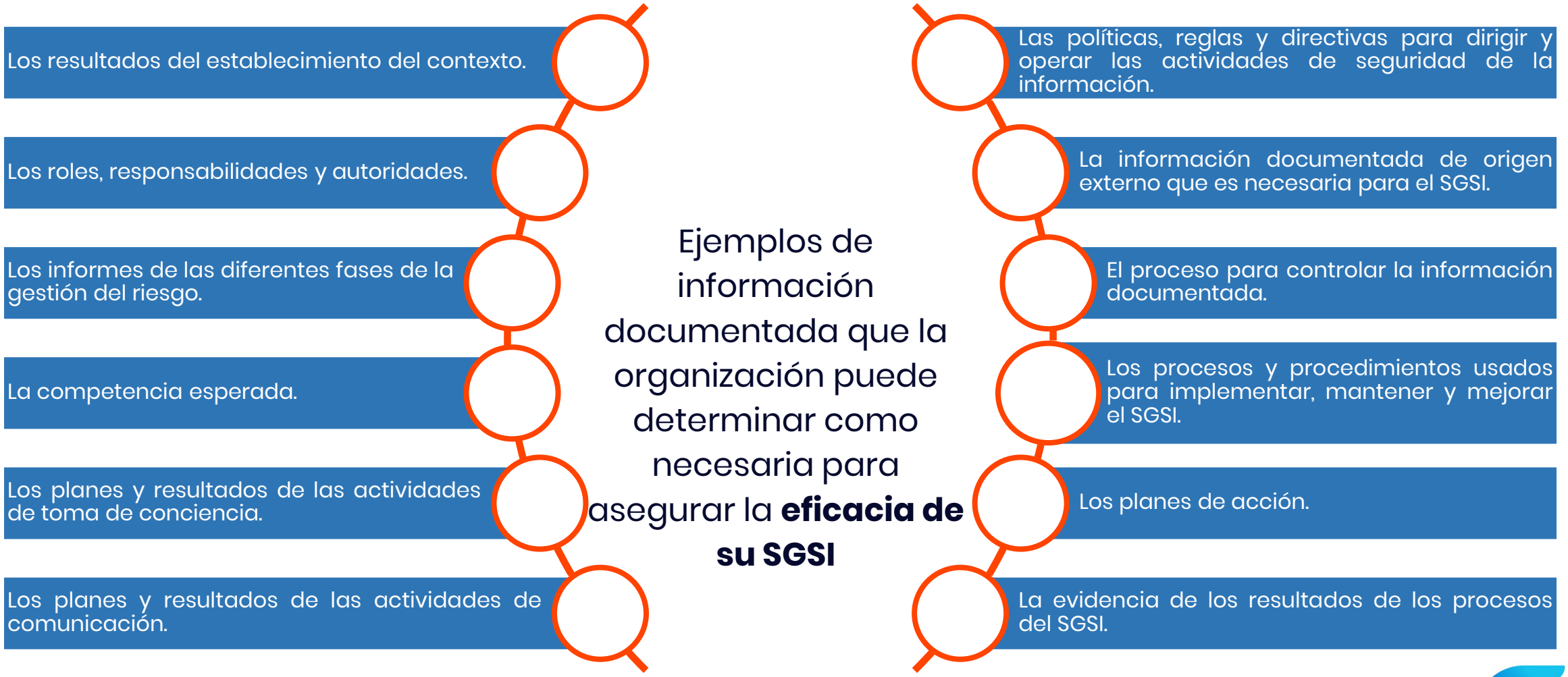
7.5.1 Información Documentada - Explicación

Hay muchas actividades dentro del SGSI que producen información documentada que se utiliza, la mayoría de el tiempo, como insumo para otra actividad.

La norma ISO IEC 27001:2022 requiere un conjunto de información documentada obligatoria y contiene un requisito general que requiere información documentada adicional si es necesaria para la eficacia del SGSI.

La cantidad de información documentada necesaria suele estar relacionada con el tamaño de la organización, la información documentada obligatoria y adicional contiene información suficiente para permitir que se lleven a cabo los requisitos de evaluación de desempeño especificados en la Cláusula 9.

7.5.1 Información Documentada - Guía



7.5.2 Creación y actualización - Requisito

Al crear y actualizar información documentada, la organización garantiza su adecuada identificación y descripción, formato y soporte, y revisión y aprobación.

7.5.2 Creación y actualización - Explicación

La organización identifica en detalle cómo se estructura mejor la información documentada y define un enfoque de documentación adecuado.

La revisión y aprobación por parte de la dirección adecuada garantiza que la información documentada sea correcta y adecuada para el propósito en forma y detalle para su objetivo.

Mediante revisiones periódicas garantizar la idoneidad y adecuación continua de la información documentada.

7.5.2 Creación y actualización - Guía

La información documentada se puede conservar tanto en papel como formulario electrónico, páginas web, bases de datos, registros informáticos, informes generados por computadora, audio y vídeo.

Además, la información documentada puede consistir en especificaciones de intención como la política de SGSI. La siguiente aplica directamente a los documentos tradicionales y debe interpretarse apropiadamente cuando aplica a otras formas de información documentada.

Las organizaciones deben crear una biblioteca de información documentada estructurada, considerando:

-determinar la estructura del marco de información documentada;
-proporcionar plantillas para diferentes tipos de información documentada;
-determinar las responsabilidades de preparar, aprobar, publicar y gestionar la información documentada; y
-determinar y documentar el proceso de revisión y aprobación para garantizar la idoneidad continua y adecuación.

7.5.2 Creación y actualización - Guía

La organización debería definir un enfoque de documentación que incluya atributos comunes de cada documento, que permiten una identificación clara y única.

Estos atributos suelen incluir **Tipo** (por ejemplo, política, directiva, regla, directriz, plan, forma, proceso o procedimiento), **el propósito y alcance ,título, fecha de publicación, clasificación, número de referencia, número de versión e historial de revisiones**, **autor y responsable(s)** del documento, su aplicación y la evolución, así como los aprobadores o la autoridad de aprobación.

Los requisitos de formato pueden incluir la definición de **lenguajes** de documentación, formatos de archivos y versión de software adecuados para trabajar con ellos y contenido gráfico. Los requisitos de medios de almacenamiento teniendo en cuenta qué información debe estar disponible.

Las declaraciones y el estilo de redacción deben adaptarse a la audiencia y al alcance de la documentación.

7.5.2 Creación y actualización – Guía

Evitar la duplicación de la información en la información documentada, y se deberían usar referencias cruzadas en lugar de repetir la misma información en diferentes
documentos.

El enfoque de documentación debe garantizar la revisión oportuna de la información documentada y que todos los cambios en la documentación están sujetos a aprobación. Los criterios de revisión adecuados pueden estar relacionados con el tiempo (p. ej. plazos máximos entre revisiones de documentos) o contenidos relacionados.

Los criterios de aprobación deben ser definidos, lo que garantiza que la información documentada sea correcta, adecuada para el propósito en forma y detalle adecuados para el público objetivo.

7.5.3 Control – Requisito

La organización gestiona la información documentada a lo largo de su ciclo de vida y la pone a disposición donde y cuando sea necesario.

7.5.3 Control – Requisito

Una vez aprobada, la información documentada se comunica a su público objetivo.

La información Documentada está disponible dónde y cuándo se necesita, preservando al mismo tiempo su integridad, confidencialidad y relevancia a lo largo de todo el ciclo de vida.

Tenga en cuenta que las actividades descritas en la norma ISO IEC 27001:2022, 7.5.3 deben realizarse si pueden realizarse y son útiles, considerando las necesidades y expectativas de la organización.

7.5.3 Control – Guía

Se puede utilizar una biblioteca de información documentada estructurada para facilitar el acceso a información documentada.

Toda la información documentada debe clasificarse de acuerdo con el esquema de clasificación de la organización, protegerse y manipulado de acuerdo con su nivel de clasificación.

Se debe garantizar que sólo personas autorizadas tienen derecho a modificarlo y distribuirlo según sea necesario a través de medios apropiados y predefinidos.

La información documentada:

-Debe protegerse para garantizar que mantenga su validez y autenticidad.

-Debe distribuirse y ponerse a disposición de las partes interesadas autorizadas.

- Debe establecer quiénes son las partes interesadas relevantes para cada uno de los casos documentados.

- Debe establecer los medios a utilizar para su distribución, acceso, recuperación y uso

- Debe cumplir con cualquier requisito relacionado con la protección y manejo de información clasificada para su distribución.

7.5.3 Control – Guía

La organización debe establecer el período de retención apropiado para la información documentada según su validez prevista y otros requisitos pertinentes.

La organización debe garantizar que la información es legible durante todo su período de retención (por ejemplo, utilizando formatos que puedan ser leídos por los usuarios disponibles, software o verificar que el papel no esté dañado).

La organización debe establecer qué hacer con la información documentada después de que su período de retención ha expirado.

La organización también debería gestionar información documentada de origen externo (es decir, de clientes, socios, proveedores, organismos reguladores, etc.).

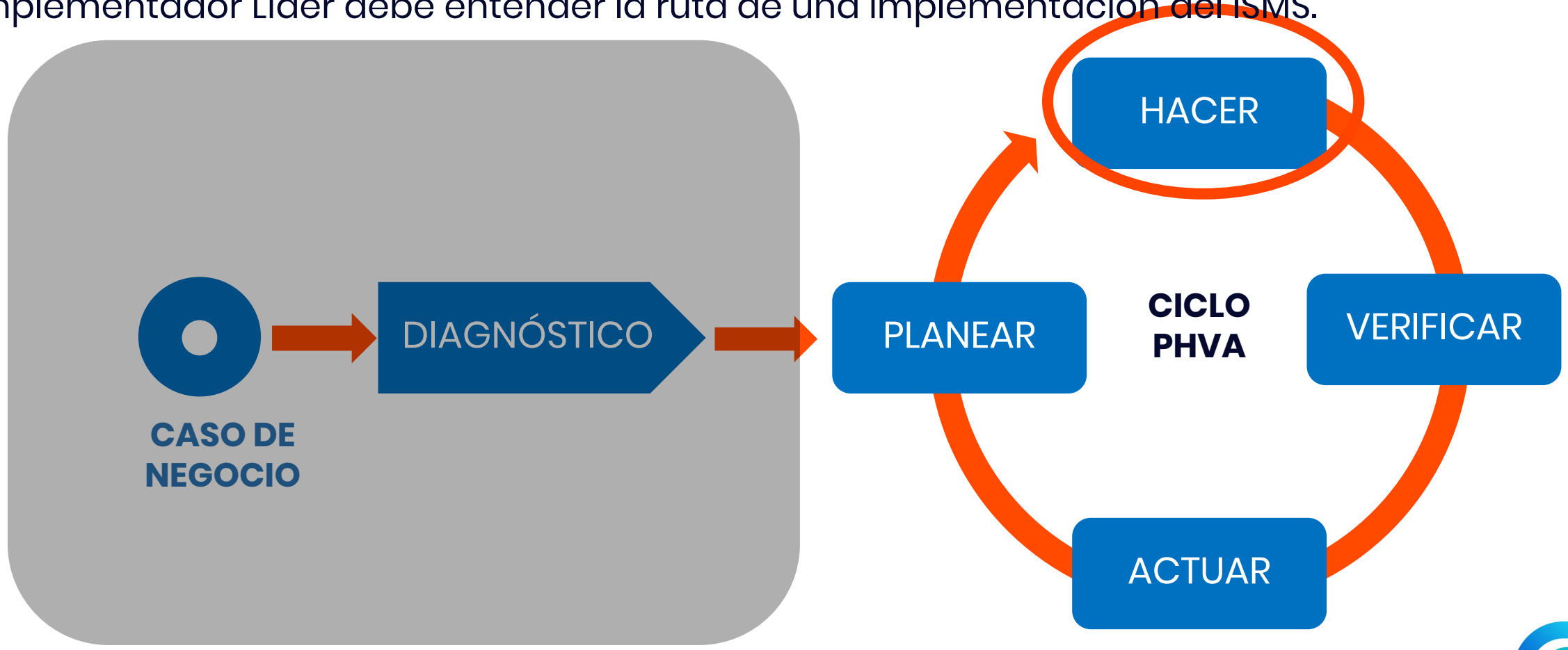
La información documentada sobre esta actividad y su resultado es obligatoria sólo en la forma y en la medida que la organización considere necesaria para la eficacia de su sistema de gestión.

8. Operación:
Interpretar los Requisitos de ISO IEC 27001

8.1 Planificación y Control Operacional
8.2 Valoración de Riesgos de Seguridad de la Información
8.3 Tratamiento de Riesgos de Seguridad de la Información

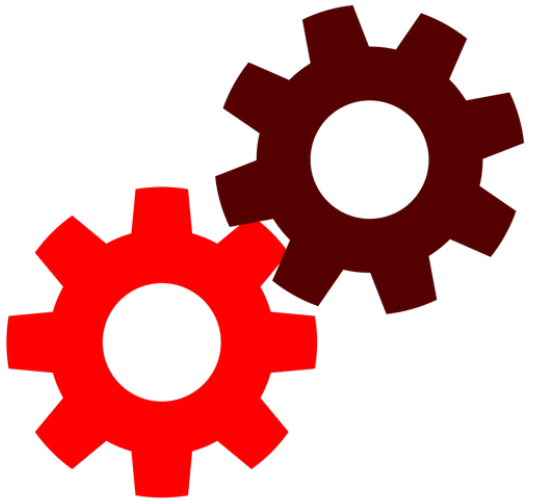
Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (hacer) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de diseñar, planificar, implementar y controlar los procesos para cumplir con su seguridad de la información.



Estructura de ISO IEC 27001

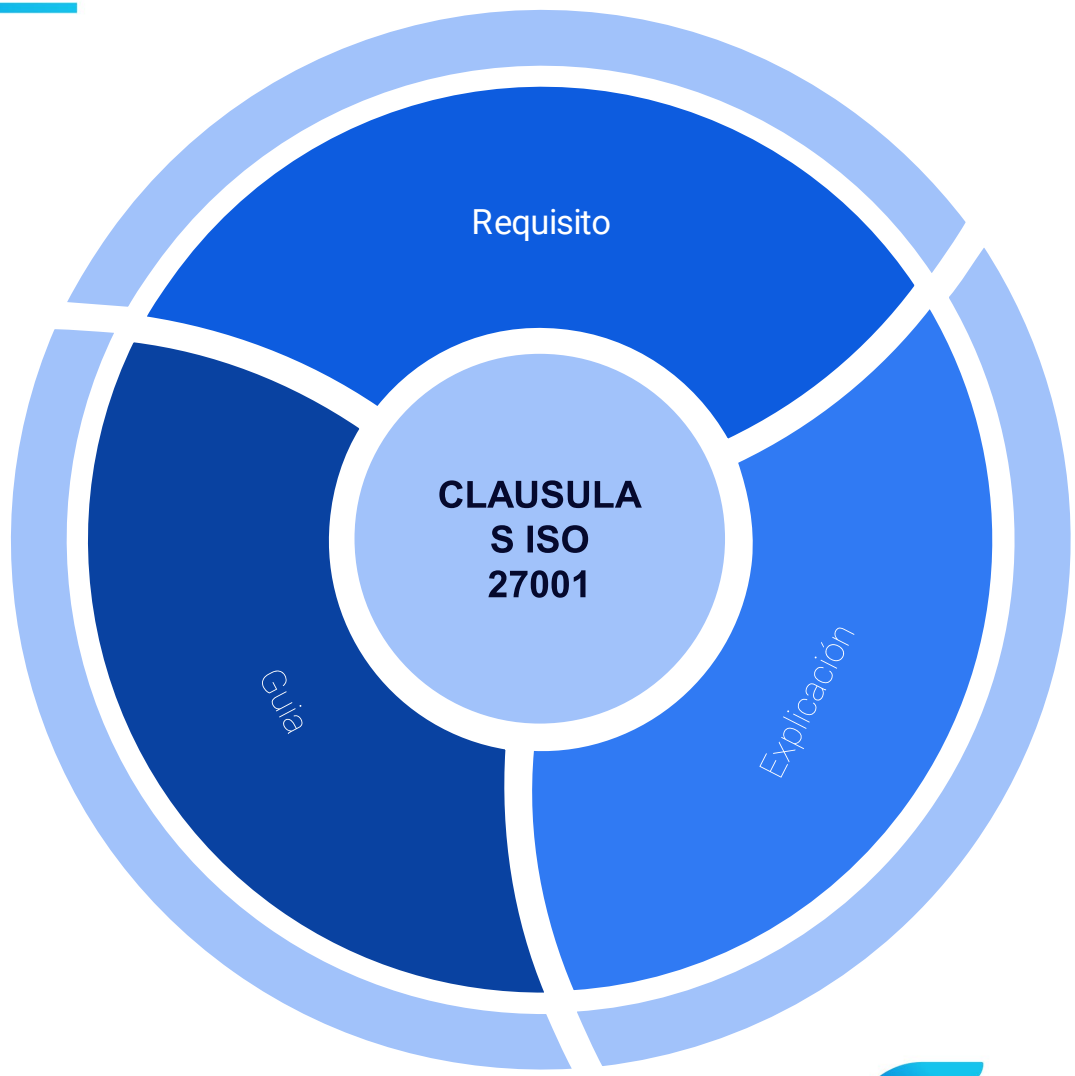
Requisitos y cómo abordarlos

En este módulo se abordan los requisitos declarados en la cláusula 8 de la ISO IEC 27001:2022 desde 3 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 8 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.



8.1 Planificación y Control Operacional - Requisito

La organización planifica, implementa y controla los proceso para cumplir con los requisitos de la seguridad de la información y alcanzar sus objetivos.

La organización mantiene información documentada según sea necesario para tener confianza en que los procesos están llevados a cabo según lo previsto.

La organización controla los cambios planificados y revisa las consecuencias de los cambios no deseados, y
garantiza que los procesos subcontratados sean identificados, definidos y controlados.

8.1 Planificación y Control Operacional - Explicación

Los procesos que utiliza una organización para cumplir con sus requisitos de seguridad de la información están planificados, y una vez implementados, se controlan, particularmente cuando se requieren cambios.

Sobre la base de la planificación del SGSI (cláusulas 6.1 y 6.2), la organización realiza las tareas necesarias, planificación operativa y actividades para implementar los procesos necesarios para cumplir con los Requisitos de la seguridad de la información.

Los procesos para cumplir con los requisitos de seguridad de la información incluyen:
a) procesos del SGSI (por ejemplo, revisión de la dirección, auditoría interna); y
b) procesos requeridos para implementar el plan de tratamiento de riesgos de seguridad de la información.

La implementación de planes da como resultado procesos operados y controlados.

En última instancia, la organización sigue siendo responsable de planificar y controlar cualquier proceso subcontratado para lograr sus objetivos de seguridad de la información.

8.1 Planificación y Control Operacional - Explicación

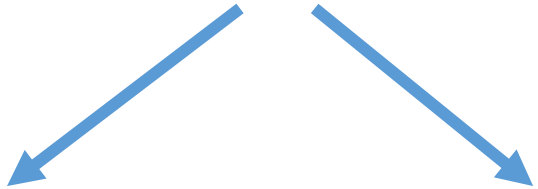
Por tanto, la organización necesita:
c) determinar los procesos subcontratados considerando los riesgos de seguridad de la información relacionados con la subcontratación; y
d) garantizar que los procesos subcontratados estén controlados (es decir, planificados, monitoreados y revisados) de manera que garantice que funcionan según lo previsto (también considerando los objetivos de seguridad y el plan de tratamiento de riesgos de seguridad de la información).

Una vez completada la implementación, los procesos se gestionan, monitorean y revisan para asegurar que continúen cumpliendo con los requisitos determinados después de comprender las necesidades y expectativas de las partes interesadas (Cláusula 4.2).

8.1 Planificación y Control Operacional - Explicación

Los cambios del SGSI pueden ser planificados u ocurrir de forma no intencionada. Siempre que la organización realiza cambios en el SGSI (como resultado de la planificación o involuntariamente), evalúa las posibles consecuencias de los cambios para controlar cualquier efecto adverso.

La organización puede obtener confianza sobre la efectividad de la implementación de los planes mediante
documentar actividades y utilizar información documentada como entrada para la evaluación del desempeño
procesos especificados en la Cláusula 9. Por lo tanto, la organización establece los requisitos de información documentada a conservar.



Planificados **No Previstos**

8.1 Planificación y Control Operacional - Guía

Los procesos que se han definido como resultado de la fase de planificación se deberían implementar, operar y verificar en toda la organización.

Se deberían considerar e implementar:

- Los procesos que son específicos para la gestión de la seguridad de la información, como gestión del riesgo, Gestión de incidentes, Gestión de la continuidad, Auditorías internas u Revisiones por la dirección.
- Los procesos que surgen de los controles de seguridad de la información en el plan de tratamiento de riesgos de seguridad de la información.
- Las estructuras de reporte dentro del área de seguridad de la información, por ejemplo, informes de incidentes, informes sobre medición del cumplimiento de los objetivos de seguridad de la información, informes sobre las actividades realizadas.
- Estructuras de reuniones (frecuencia, participantes, propósito y autorización) dentro de la información. Las actividades de seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes para una gestión eficaz del área de seguridad de la información.

8.1 Planificación y Control Operacional - Guía

Cambios Planificados

La organización debería:

- **Planificar** su implementación y asignar tareas, responsabilidades, fechas límite y recursos.
- **Implementar** cambios de acuerdo con el plan.
- **Hacer seguimiento** de su implementación para confirmar que se han implementado de acuerdo con el plan.
- **Recolectar y retener** información documentada sobre la ejecución de los cambios como evidencia de que se han llevado a cabo de la forma planificada (por ejemplo, con responsabilidades, fechas límite, evaluaciones de eficacia).

8.1 Planificación y Control Operacional - Guía

Cambios No Previstos

La organización debería:

- **Examinar** sus consecuencias.
- **Determinar** si ya ha ocurrido algún efecto adverso o puede ocurrir en el futuro.
- **Planificar e implementar** acciones para mitigar cualquier efecto adverso, de acuerdo con las necesidades.
- **Recolectar y conservar** información documentada sobre cambios y acciones no previstos tomados para mitigar los efectos adversos.

8.1 Planificación y Control Operacional - Guía

Procesos o Funciones Controlados con Proveedores Externos

La organización debería:

- **Determinar** todas las relaciones de contratación externa.
- **Establecer** las interfaces apropiadas con los proveedores.
- **Abordar** las cuestiones relacionadas con seguridad de la información, en los acuerdos con proveedores.
- **Hacer seguimiento y revisar** los servicios de los proveedores para asegurar que operan en la forma prevista y que los riesgos de seguridad de la información asociados satisfacen los criterios de aceptación de riesgos de la organización.
- **Gestionar** los cambios a los servicios de los proveedores, de acuerdo con las necesidades.

8.2 Evaluación de Riesgos de Seguridad de la Información – Requisito

La organización realiza evaluaciones de riesgos de seguridad de la información y conserva información documentada.

RISK

8.2 Evaluación de Riesgos de Seguridad de la Información – Explicación

Cuando se llevan a cabo evaluaciones de riesgos de seguridad de la información, la organización ejecuta el proceso de valoración de riesgos establecido en la fase de Planificación.

La organización debería:

- Contar con **un plan para llevar a cabo las evaluaciones de riesgos** de seguridad de la información programadas cuando ocurran cambios significativos en el SGSI (o en su contexto) o incidentes de seguridad de la información.
- Determinar cuáles de estos cambios o incidentes requieren una evaluación adicional de los riesgos de seguridad de la información.
- Determinar cómo se desencadenan estas evaluaciones.
- Perfeccionar gradualmente el nivel de detalle de la identificación de riesgos en repeticiones posteriores de la evaluación de riesgos de seguridad de la información en el contexto de la mejora continua del SGSI.
- Llevar a cabo una evaluación de riesgos de seguridad de la información al menos una vez al año.

8.3 Tratamiento de Riesgos de Seguridad de la Información - Requisito

La organización implementa el plan de tratamiento de riesgos de seguridad de la información y conserva información documentada sobre los resultados del tratamiento de seguridad de la información.

CÓDIGO RIESGO	DESCRIPCIÓN	NIVEL DE RIESGO	PROCESO DE NEGOCIO	ACTIVOS RELACIONADOS	ESTRATEGIA	ACCIONES A DESARROLLAR	CONTROL DE REFERENCIA ANEXO A	TIPO DE CONTROL	RESPONSABLE	PLAZO

8.3 Tratamiento de Riesgos de Seguridad de la Información - Explicación

Para tratar los riesgos de seguridad de la información, la organización necesita llevar a cabo las medidas de seguridad de la información del proceso de tratamiento de riesgos definido en 6.1.3.

Durante la operación del SGSI, siempre que la evaluación de riesgos se actualiza de acuerdo con 8.2, la organización luego aplica el tratamiento de riesgos de acuerdo con 6.1.3 y actualiza el plan de tratamiento de riesgos. Se implementa nuevamente el plan de tratamiento de riesgos actualizado.

Los resultados del tratamiento de riesgos de seguridad de la información se conservan en información documentada como evidencia de que el proceso en 6.1.3 se ha realizado según lo definido.

8.3 Tratamiento de Riesgos de Seguridad de la Información – Guía

El proceso de tratamiento de riesgos de seguridad de la información debe realizarse después de cada iteración del proceso de evaluación de seguridad de la información en 8.2 o cuando la implementación del plan de tratamiento de riesgos o partes de él fallan.

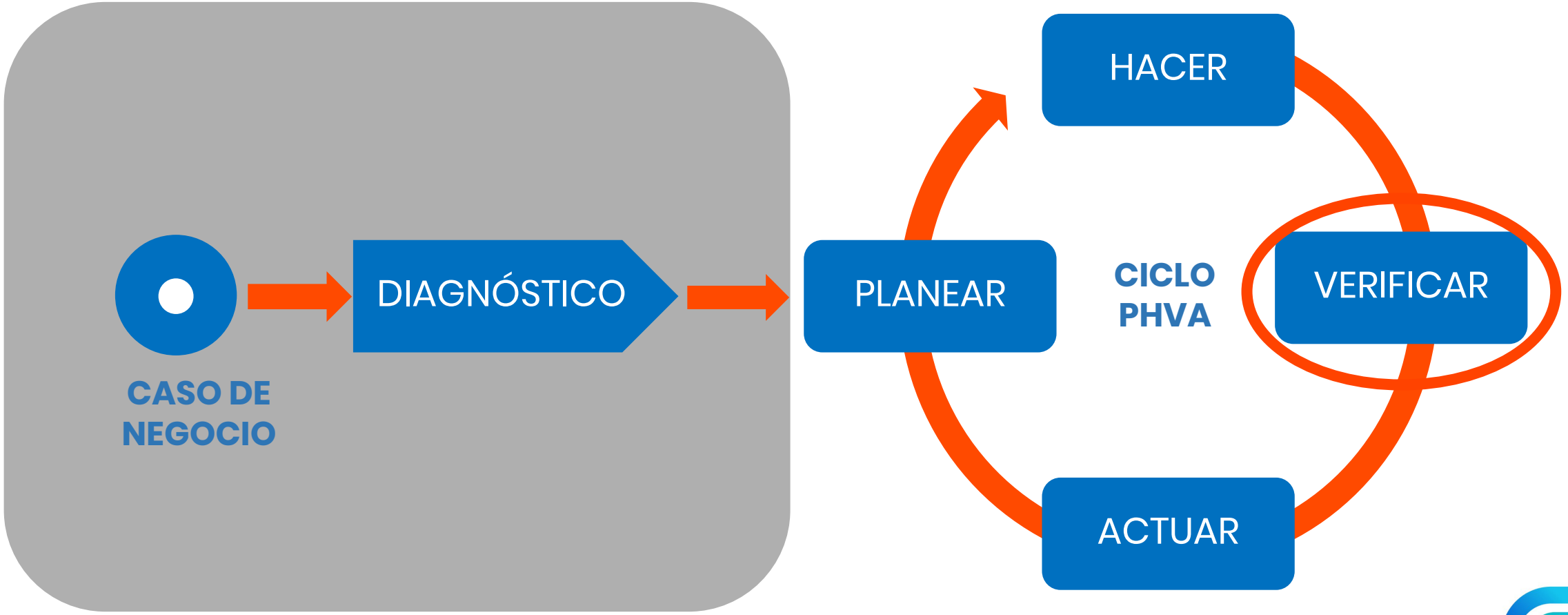
El progreso de la implementación del plan de tratamiento de riesgos de seguridad de la información debe ser impulsado y monitoreados por esta actividad.

9. Evaluación del Desempeño: Interpretar los Requisitos de ISO IEC 27001

9.1 Seguimiento, Medición, Análisis y Evaluación
9.2 Auditoría Interna
9.3 Revisión por la Dirección

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (verificar) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de diseñar mecanismos de seguimiento, medición, análisis y evaluación del ISMS a la vez que deberá conocer los componentes de una auditoría ISO IEC 27001:2022 interna.

Estructura de ISO IEC 27001

Requisitos y cómo abordarlos

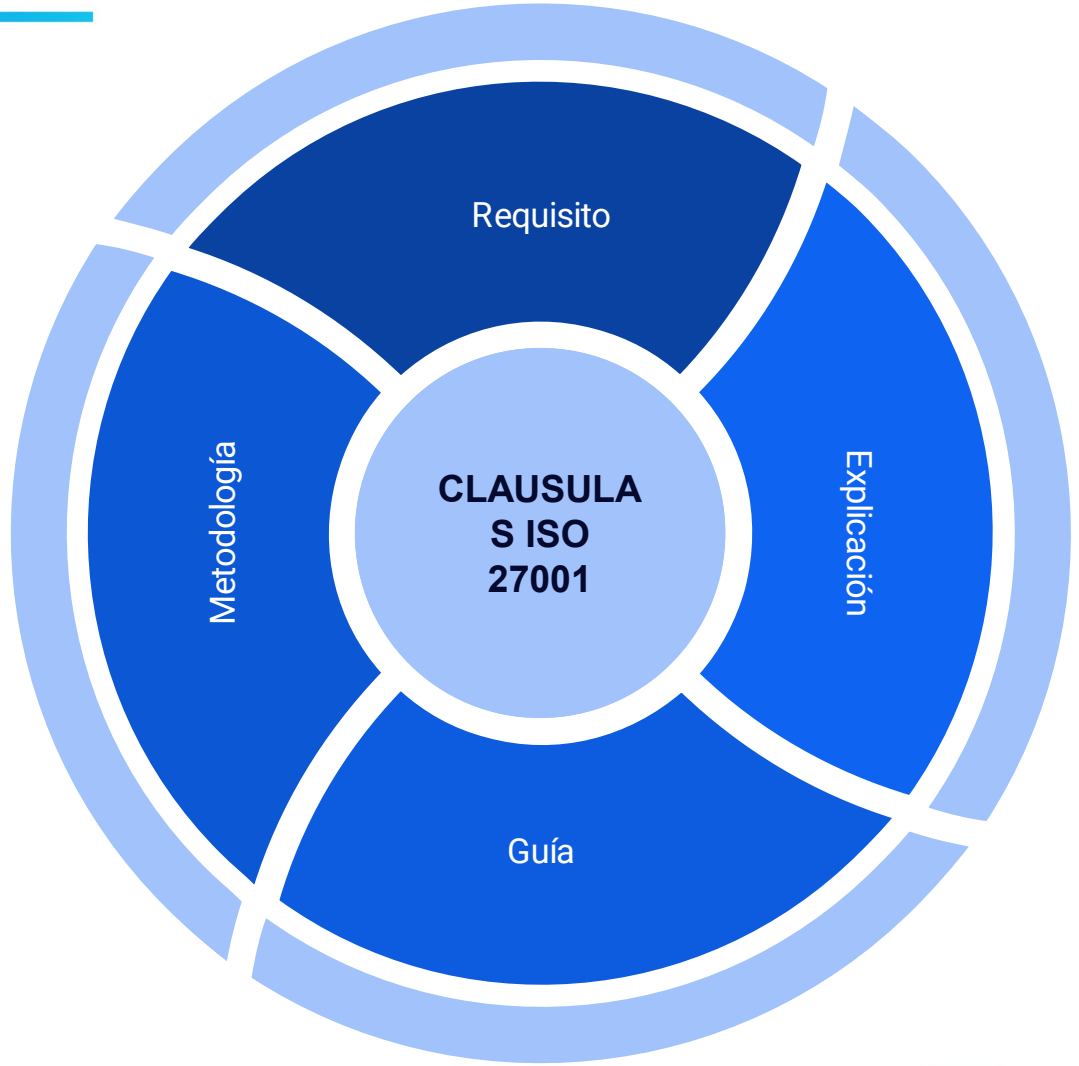
En este módulo se abordan los requisitos declarados en la cláusula 9 de la ISO IEC 27001:2022 desde 4 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 9 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Metodología: Serie de métodos, técnicas, mejores prácticas y pasos recomendados para abordar los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarados en la cláusula 9 de la ISO 27001 (se incluye para el tema definido en el alcance del módulo).



9.1 Seguimiento, Medición, Análisis y Evaluación - Requisito

SEGUIMIENTO Y MEDICIÓN

La organización evalúa el desempeño de la seguridad de la información y la efectividad del SGSI.

9.1 Seguimiento, Medición, Análisis y Evaluación - Explicación

SEGUIMIENTO Y MEDICIÓN

Ayudar a la organización a juzgar si el resultado previsto de las actividades de la seguridad de la información, incluidas la evaluación y el tratamiento de los riesgos, se han logrado en la forma prevista.

- A qué hacer seguimiento y qué medir.
- Quién hace el seguimiento, quién mide y cuándo lo hace.
- Los métodos para obtener resultados válidos (es decir, comparables y reproducibles).

9.1 Seguimiento, Medición, Análisis y Evaluación – Explicación

ANÁLISIS Y EVALUACIÓN

La Organización Establece

Objetivo

- Quién establece y evalúa los resultados del seguimiento y la medición, y cuándo.
- Los métodos para producir resultados válidos. Existen dos aspectos de la evaluación.

Del Desempeño

De la eficacia del SGSI

La Organización Establece

Para determinar si la organización tiene el desempeño esperado, lo cual incluye determinar en qué medida los procesos dentro del SGSI cumplen sus especificaciones.

Para determinar si la organización está haciendo las cosas de una manera adecuada, lo que incluye determinar en qué medida se cumplen los objetivos de la seguridad de la información.

9.1 Seguimiento, Medición, Análisis y Evaluación - Guía

ASPECTOS A MEDIR

Una buena práctica es definir la "necesidad de información" al planificar el seguimiento, medición, análisis y evaluación.

Una necesidad de información generalmente se expresa como un alto nivel de seguridad de la información, pregunta o declaración que ayuda a la organización a evaluar el desempeño de la seguridad de la información y la eficacia del SGSI.

En otras palabras, se debe realizar seguimiento y medición para lograr un objetivo definido, se debe tener cuidado al determinar los atributos a medir. Es impracticable, costoso y contraproducente medir demasiado o elegir los atributos incorrectos.

Existen dos tipos genéricos de medidas:

mediciones de desempeño, que expresan los resultados planificados en términos de las características de la actividad planificada, como el recuento de personas, el logro de hitos o el grado en que se implementan los controles de seguridad de la información; y

mediciones de efectividad, que expresan el efecto que tiene la realización de las actividades planificadas sobre los objetivos de seguridad de la información de la organización.

9.1 Seguimiento, Medición, Análisis y Evaluación - Guía

ASPECTOS A MEDIR

- Avance del proyecto de Implementación
- Disminución del valor del riesgo de un período a otro
- Cubrimiento del presupuesto asignado
- Mejoramiento en la percepción de seguridad de las partes interesadas
- Conocimiento de la política
- Disminución de incidentes de seguridad en confidencialidad, integridad o disponibilidad
- Atención de incidentes
- Eficacia de las acciones correctivas
- Lecciones aprendidas implementadas
- Evaluación del personal
- Disminución de No conformidades identificadas por proceso
- Verificación de condiciones de seguridad en teletrabajo
- Tiempo de demora en el retiro de privilegios
- Eficacia en el mantenimiento de equipos
- Incidentes por asignación y manejo de contraseñas
- Equipos que salen e ingresan de la organización
- Medios extraíbles controlados
- Recuperaciones del backup
- Eficacia en el cumplimiento de las evacuaciones y de los simulacros
- Amenazas detectadas por antivirus
- Disminución de vulnerabilidades técnicas identificadas de un período a otro

9.2 Auditoría Interna - Requisito

La organización realiza auditorías internas para proporcionar información sobre la conformidad del SGSI con los requisitos.

9.2 Auditoría Interna - Explicación

La evaluación de un SGSI a intervalos planificados mediante auditorías internas proporciona seguridad del estado del SGSI a la alta dirección. **La auditoría se caracteriza por una serie de principios: integridad; presentación justa ; debido cuidado profesional; confidencialidad; independencia; y un enfoque basado en la evidencia.** (ver ISO 19011).

Las auditorías internas proporcionan información sobre si el SGSI se ajusta a los propios estándares de la organización, así como los requisitos de ISO IEC 27001:2022.

Los requisitos incluyen:

a) requisitos establecidos en la política y los procedimientos de seguridad de la información;

b) requisitos producidos por el marco para establecer objetivos de seguridad de la información, incluyendo resultados del proceso de tratamiento de riesgos;

c) requisitos legales y contractuales; y

d) requisitos sobre la información documentada.

9.2 Auditoría Interna - Explicación

Los auditores también evalúan si el SGSI se implementa y mantiene efectivamente

PROGRAMA DE AUDITORÍA

Describe el marco general para un grupo de auditorías planificadas para tiempos específicos y dirigidas hacia propósitos específicos.

PLAN DE AUDITORÍA

Describe las actividades y disposiciones para una auditoría específica.

CRITERIOS DE AUDITORÍA

Son un conjunto de políticas, procedimientos o requisitos usados como referencia contra los cuales se compara la evidencia de auditoría, es decir, los criterios de auditoría describen lo que los auditores esperan encontrar.

9.2 Auditoría Interna - Guía

Gestionar un programa de auditoría

Un programa de auditoría define la estructura y las responsabilidades para planificar, realizar y presentar informes, y finalmente dar seguimiento a las actividades de auditoría individuales. Como tal, debería garantizar que las auditorías realizadas tengan el alcance adecuado, minimicen el impacto en las operaciones de la organización y mantengan la calidad necesaria de las auditorías.

Un programa de auditoría también debería garantizar la competencia de equipos de auditoría, el mantenimiento adecuado de los registros de auditoría, seguimiento y revisión de las operaciones, riesgos y eficacia de las auditorías. Además, un programa de auditoría debe garantizar que el SGSI (es decir, todos procesos, funciones y controles relevantes) se audita dentro de un período de tiempo específico.

El programa debe incluir información documentada sobre tipos, duración, ubicaciones y cronograma de las auditorías.

El alcance y la frecuencia de las auditorías internas deben basarse en el tamaño y la naturaleza de la organización, así como de la naturaleza, funcionalidad, complejidad y nivel de madurez del SGSI (basado en riesgos).

9.2 Auditoría Interna - Guía

La eficacia de los controles implementados debe examinarse en el ámbito de las auditorías internas.

Se debe diseñar un programa de auditoría para garantizar la cobertura de todos los controles necesarios e incluir la evaluación de la eficacia de los controles seleccionados a lo largo del tiempo. Controles clave (según el programa de auditoría) deben incluirse en cada auditoría, mientras que se deben implementar controles para gestionar niveles más bajos.

El programa de auditoría también debe considerar que los procesos y controles deberían haber estado en funcionamiento durante algún tiempo para permitir la evaluación de pruebas adecuadas.

Las auditorías internas relativas a un SGSI se pueden realizar eficazmente como parte de, o en colaboración con, otras auditorías internas de la organización. El programa de auditoría puede incluir auditorías relacionadas con uno o más estándares de sistemas de gestión, realizados por separado o en combinación.

Un programa de auditoría debe incluir información documentada sobre: criterios de auditoría, métodos de auditoría, selección de equipos de auditoría, procesos para el manejo de la confidencialidad, seguridad de la información y disposiciones para auditores.

9.2 Auditoría Interna - Guía

Competencia y evaluación de los auditores.

En cuanto a la competencia y evaluación de los auditores, la organización debería:

- Identificar los requisitos de competencia para sus auditores;
- Seleccionar auditores internos o externos con la competencia adecuada;
- Contar con un proceso para monitorear el desempeño de los auditores y equipos de auditoría;
- Incluir personal en los equipos de auditoría interna que tengan información y sectores específicos apropiados.
- Contar con conocimientos de seguridad.

Los auditores deben seleccionarse teniendo en cuenta que deben ser competentes, independientes y adecuadamente entrenado.

Seleccionar auditores internos puede resultar difícil para las empresas más pequeñas. Si los recursos necesarios y si las competencias no están disponibles internamente, se deberían nombrar auditores externos.

9.2 Auditoría Interna - Guía

Cuando las organizaciones decidan utilizar auditores externos, estos deben asegurarse de que hayan adquirido suficiente conocimiento sobre el contexto de la organización. Esta información debe ser suministrada por personal interno.

Las organizaciones deben considerar que los empleados internos que actúan como auditores internos pueden ser capaces de realizar auditorías detalladas considerando el contexto de la organización, pero es posible que no tengan suficiente conocimiento sobre la realización de auditorías.

Las organizaciones deberían reconocer las características y posibles deficiencias de los procesos internos versus los auditores externos y establecer equipos de auditoría adecuados con el conocimiento y la competencia necesarios.

9.2 Auditoría Interna - Guía

Realización de la auditoría

Al realizar la auditoría, el líder del equipo auditor debe preparar un plan de auditoría considerando los resultados de auditorías previas y la necesidad de dar seguimiento a las no conformidades reportadas previamente y a las normas inaceptables.

El plan de auditoría debe conservarse como información documentada y debe incluir criterios, alcance y métodos de la auditoría.

El equipo auditor debe revisar:

— adecuación y eficacia de los procesos y controles determinados;

— cumplimiento de los objetivos de seguridad de la información;

— cumplimiento de los requisitos definidos en ISO IEC 27001:2022, cláusulas 4 a 10;

— cumplimiento de los requisitos de seguridad de la información propios de la organización;

— coherencia de la Declaración de Aplicabilidad con el resultado del riesgo de seguridad de la información y el proceso de tratamiento;

— coherencia del plan de tratamiento de riesgos de seguridad de la información real con los riesgos evaluados identificados y los criterios de aceptación de riesgos;

9.2 Auditoría Interna - Guía

— relevancia (teniendo en cuenta el tamaño y la complejidad de la organización) de los aportes de la revisión por la dirección , salidas; y

— impactos de los resultados de la revisión por la dirección (incluidas las necesidades de mejora) en la organización.

El alcance y la confiabilidad del monitoreo disponible sobre la efectividad de los controles producidos por el SGSI (ver 9.1) puede permitir a los auditores reducir sus propios esfuerzos de evaluación,

Si el resultado de la auditoría incluye no conformidades, el auditado debe preparar un plan de acción para cada no-conformidad a ser acordada con el líder del equipo auditor.

Un plan de acción de seguimiento normalmente incluye:

i) descripción de la no conformidad detectada;

j) descripción de la(s) causa(s) de la no conformidad;

k) descripción de la corrección a corto y largo plazo para eliminar un problema detectado o no-conformidad dentro de un plazo definido; y

l) las personas responsables de la ejecución del plan.

9.2 Auditoría Interna - Guía

Los informes de auditoría, con los resultados de la auditoría, deben distribuirse a la alta dirección.

Se deben revisar los resultados de las auditorías anteriores y ajustar el programa de auditoría para gestionar mejor las áreas que experimentan mayores riesgos debido a no conformidades.

Recomendación


INTERNATIONAL STANDARD

ISO 19011

Third edition
2018-07

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

ISO

Reference number
ISO 19011:2018(E)

© ISO 2018

Se recomienda consultar la norma ISO 19011:2018 para mayor orientación sobre cómo ejecutar auditorías a sistemas de gestión, esta norma da orientación sobre los principios de auditoría, la gestión de un programa de auditoría y la realización de auditorías del sistema de gestión, así como orientación sobre la evaluación de la competencia de las personas involucradas en el proceso de auditoría.

9.2 Auditoría Interna - Metodología

Estas actividades incluyen las personas que administran el programa de auditoría, los auditores y los equipos de auditoría.

Es aplicable a todas las organizaciones que necesitan planificar y llevar cabo auditorías internas o externas de los sistemas de gestión o administrar un programa de auditoría.

La aplicación de este documento a otros tipos de auditorías es posible, siempre que se otorgue una consideración especial a la competencia específica necesaria.

9.2 Auditoría Interna - Metodología

Estructura de la norma ISO 19011:2018

Prefacio
Introducción
1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Principios de auditoría
5. Administrar de un programa de auditoría
6. Realización de una auditoría.
7. Competencia y evaluación de los auditores

Anexo A
Bibliografía

9.2 Auditoría Interna - Metodología

Auditoría:

- Proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría

- **Nota 1:** las auditorías internas, a veces llamadas auditorías de primera parte, son realizadas por, o en nombre de, la organización misma

- **Nota 2:** Las auditorías externas incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por las partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales

9.2 Auditoría Interna – Metodología

TABLA 1 - DIFERENTES TIPOS DE AUDITORÍA

Auditoría de Primera Parte	Auditoría de Segunda Parte	Auditoría de Tercera Parte
AUDITORÍA INTERNA	Auditoría de proveedor externo.	Auditoría de certificación y/o acreditación.
	Otra auditoría de parte interesada externa.	Auditoría legal, regulatoria y similar.

9.2 Auditoría Interna – Metodología

Los criterios de auditoría:

Son un conjunto de requisitos utilizados como referencia con respecto a los cuales se compara la evidencia objetiva.

Nota 1: Si los criterios de auditoría son legales (incluidos los requisitos legales o reglamentarios), las palabras “cumplimiento” o “incumplimiento” a menudo se utilizan en una conclusión de auditoría.

Nota 2: Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, etc.

9.2 Auditoría Interna – Metodología

La evidencia:

- La evidencia objetiva son los datos que respaldan la existencia o la verdad de algo
- **Nota 1**: La evidencia objetiva se puede obtener a través de observación, medición, prueba o por otros medios
- **Nota 2:** La evidencia objetiva para el propósito de la auditoría generalmente consiste en registros, declaraciones de hechos u otra información que son relevantes para los criterios de auditoría y verificables

9.2 Auditoría Interna - Metodología

Los resultados de la evaluación de la evidencia de auditoría recopilada contra los criterios de auditoría

- **Nota 1:** Los hallazgos de la auditoría indican conformidad o no conformidad
- **Nota 2:** Los hallazgos de la auditoría pueden conducir a la identificación de riesgos, oportunidades de mejora o registro de buenas prácticas
- **Nota 3:** En inglés, si los criterios de auditoría se seleccionan entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o incumplimiento

9.2 Auditoría Interna - Metodología

Conclusiones de auditoría:

Resultado de una auditoría después de considerar los objetivos de auditoría y todos los resultados (hallazgos) de auditoría.

9.3 Revisión por la Dirección - Requisito

La alta dirección revisa el SGSI a intervalos planificados.

9.3 Revisión por la Dirección - Requisito

El propósito de la revisión por la dirección es garantizar la idoneidad, adecuación y eficacia continua del SGSI.

La idoneidad se refiere a la alineación continua con los objetivos de la organización.

Adecuación y eficacia se refieren a un diseño adecuado y a la integración organizativa del SGSI, así como a la Implementación efectiva de procesos y controles impulsados por el SGSI.

En general, la revisión por la dirección es un proceso que se lleva a cabo en varios niveles de la organización.

Las actividades pueden variar desde reuniones diarias, semanales o mensuales de la unidad organizacional hasta informes simples. La alta dirección es en última instancia responsable de la revisión, con aportes de todos los niveles en la organización.

9.3 Revisión por la Dirección – Guía

La alta dirección debe exigir y revisar periódicamente los informes sobre el desempeño del SGSI.
Hay muchas maneras en que la gerencia puede revisar el SGSI, como recibir y revisar mediciones e informes, comunicación electrónica, actualizaciones verbales.
Los insumos clave son los resultados de las medidas de seguridad de la información descritas en 9.1, los resultados de las auditorías internas descrito en 9.2 y los resultados de la evaluación de riesgos con el estado del plan de tratamiento de riesgos. Al revisarlos debe confirmar que los riesgos residuales cumplen con los criterios de aceptación, que el plan de tratamiento aborda todos los riesgos relevantes y sus opciones de tratamiento.
Todos los aspectos del SGSI deben ser revisados por la dirección a intervalos planificados, Estableciendo horarios y puntos del orden del día adecuados en las reuniones de gestión.

La agenda de la revisión por la dirección debe abordar los siguientes temas:

Agenda

- Resultados de Revisiones anteriores.
- Retroalimentación de las partes interesadas.
- Cambios externos e internos.
- Desempeño de procesos.
- No conformidades y acciones correctivas.
- Seguimiento y resultados de mediciones.
- Resultados de Auditorías.
- Cumplimiento de objetivos.
- Resultados de evaluación de riesgos y estado del plan de tratamiento.
- Comentarios de las partes interesadas.
- Oportunidades de mejora.

9.3 Revisión por la Dirección – Guía

Los aportes a la revisión por parte de la dirección deben tener el nivel apropiado de detalle, de acuerdo con los objetivos establecidos para la dirección involucrada en la revisión.

Los resultados del proceso de revisión por la dirección deben incluir:

Decisiones relacionadas con la evaluación continua oportunidades de mejora y cualquier necesidad de cambios en el SGSI.

Se requiere información documentada de las revisiones de la dirección.

Debe conservarse para demostrar que se haya tenido en cuenta la agenda, incluso cuando sea decidido que no es necesaria ninguna acción.

Cuando se realizan varias revisiones de la gestión en diferentes niveles de la organización, entonces se deben ser vinculados entre sí de manera apropiada.

Evidencia de decisiones relativas a:

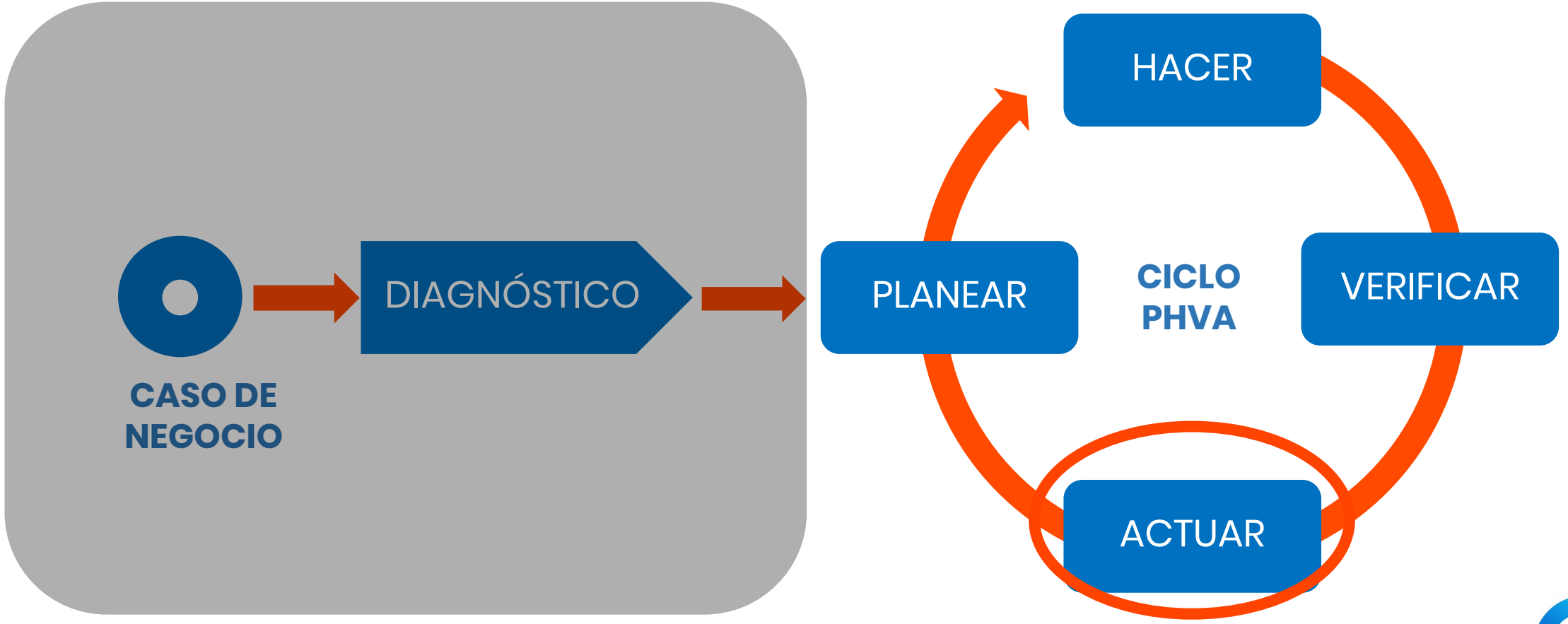
- Cambios en la política y los objetivos de seguridad de la información.
- Cambios en los criterios de aceptación de riesgos y en los criterios para realizar riesgos de seguridad de la información
- Acciones, si es necesario, luego de la evaluación del desempeño de la seguridad de la información.
- Cambios de recursos o presupuesto del SGSI;
- Plan de tratamiento de riesgos actualizado
- Mejoras de las actividades de seguimiento y medición.

10. Mejora:
Interpretar los Requisitos de ISO IEC 27001

10.1 No Conformidad y Acción Correctiva
10.2 Mejora Continua

Objetivo de la ruta de navegación

El candidato a la certificación de ISO IEC 27001:2022 Implementador Líder comprenderá la segunda fase (Actuar) de la ruta de implementación de la norma ISO IEC 27001:2022, como Implementador Líder debe entender la ruta de una implementación del ISMS.



Objetivo del Módulo

Al finalizar este módulo el candidato a la certificación de ISO IEC 27001:2022 Implementador Líder debe estar en capacidad de actuar ante las no conformidades.

Estructura de ISO IEC 27001

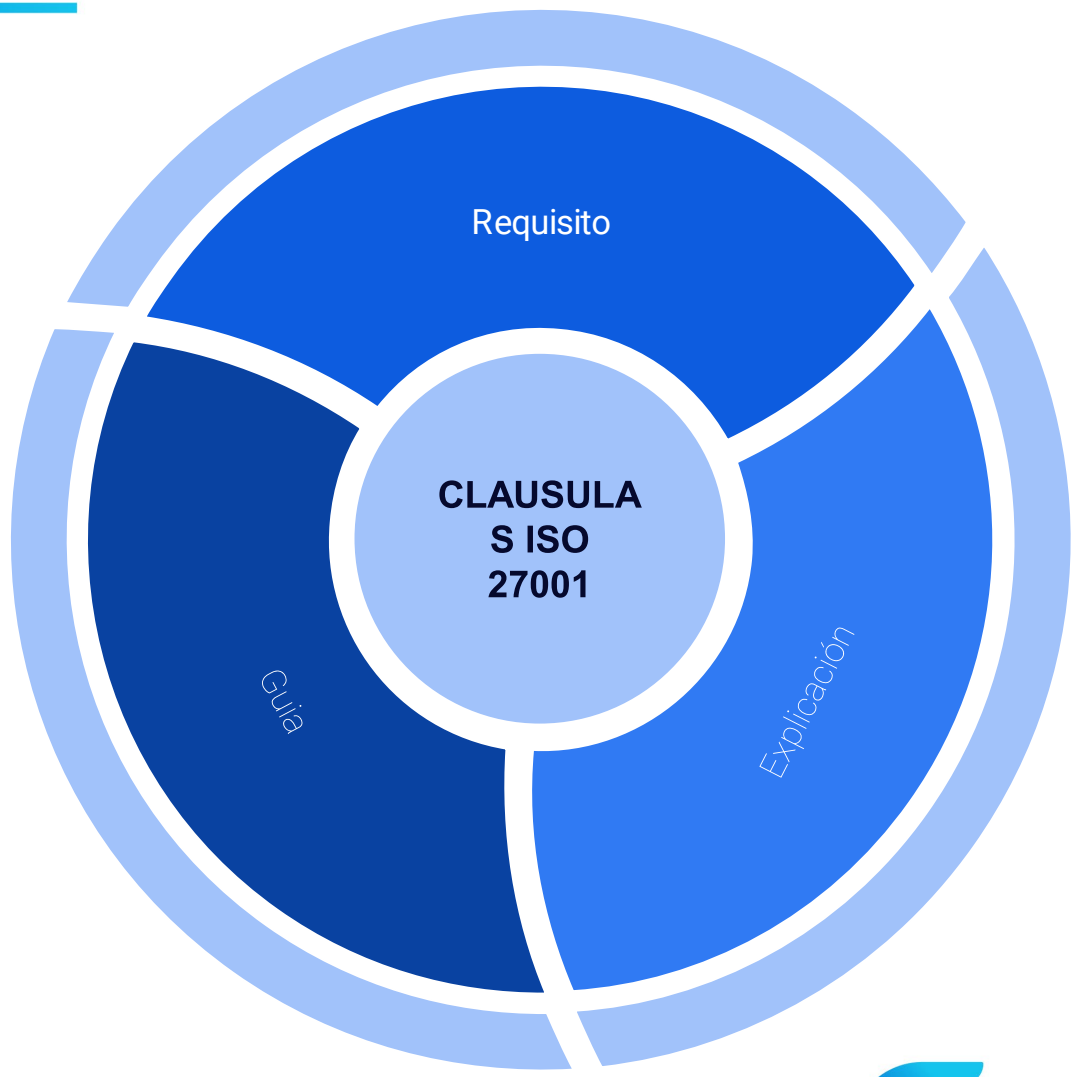
Requisitos y cómo abordarlos

En este módulo se abordan los requisitos declarados en la cláusula 10 de la ISO IEC 27001:2022 desde 3 perspectivas:

Requisito: Identifica los requisitos de cumplimiento para un sistema de gestión de seguridad de la información declarado en la cláusula 10 de la ISO 27001.

Explicación: Proporciona una explicación sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.

Guía: Proporciona orientación y recomendaciones sobre los requisitos de cumplimiento para un sistema de gestión de seguridad de la información por la ISO 27003.



10.1 No Conformidad y Acción Correctiva - Requisito

La organización reacciona ante las no conformidades, las evalúa y toma acciones correctivas si es necesario.

10.1 No Conformidad y Acción Correctiva - Explicación

Una no conformidad es el incumplimiento de un requisito del SGSI. Los requisitos son necesidades o expectativas declaradas, implícitas u obligatorias.

Existen varios tipos de no conformidades como:

a) Incumplimiento de un requisito (total o parcialmente) de la norma ISO/IEC 27001 en el SGSI;
b) No implementar correctamente o no cumplir con un requisito, regla o control establecido por el SGSI; y
c) Incumplimiento parcial o total de requisitos legales, contractuales o pactados con el cliente.

Las no conformidades pueden ser, por ejemplo:
d) Personas que no se comportan como se espera según los procedimientos y políticas;
e) Proveedores que no proporcionan productos o servicios acordados;
f) Proyectos que no arrojan los resultados esperados; y
g) Controles que no funcionan según el diseño.

10.1 No Conformidad y Acción Correctiva - Explicación

Las no conformidades pueden reconocerse mediante:

h) deficiencias de las actividades realizadas en el ámbito del sistema de gestión;
i) controles ineficaces que no se remedian adecuadamente;
j) análisis de incidentes de seguridad de la información, que demuestre el incumplimiento de un requisito del SGSI;
k) quejas de los clientes;
l) alertas de usuarios o proveedores;
m) resultados de seguimiento y medición que no cumplan con los criterios de aceptación; y
n) objetivos no alcanzados.

10.1 No Conformidad y Acción Correctiva - Guía

Los incidentes de seguridad de la información no implican necesariamente que exista una no conformidad, pero pueden ser un indicador de una no conformidad. La auditoría interna y externa y las quejas de los clientes son otros aspectos importantes en la identificación de no conformidades.

La reacción a la no conformidad debe basarse en un proceso de manejo definido. El proceso debe incluir:
— identificar el alcance y el impacto de la no conformidad;
— decidir sobre las correcciones para limitar el impacto de la no conformidad;
— comunicarse con el personal pertinente para garantizar que se lleven a cabo las correcciones;
— realizar las correcciones que se decidan;
— supervisar la situación para garantizar que las correcciones hayan tenido el efecto deseado y no produjo efectos secundarios no deseados;
— actuar más para corregir la no conformidad si aún no se remedia; y
— comunicarse con otras partes interesadas relevantes, según corresponda.

Como resultado general, el proceso de manejo debe conducir a un estado gestionado con respecto a la no conformidad y las consecuencias asociadas.

Sin embargo, las correcciones por sí solas no necesariamente evitarán la recurrencia de la no conformidad.

10.1 No Conformidad y Acción Correctiva - Guía

ACCIONES CORRECTIVAS

Están dirigidas a eliminar la causa de una no conformidad y a evitar su recurrencia. Las acciones correctivas pueden ocurrir después de las correcciones o paralelas a ellas.

Tipos

Se deberían emprender los siguientes pasos del proceso:

1. Decidir si es necesario llevar a cabo una acción correctiva de acuerdo con los criterios establecidos.
2. Revisar la no conformidad considerando si se han registrado no conformidades similares, todas las consecuencias y sus efectos secundarios causados, y las correcciones realizadas.
3. Realizar un análisis a fondo de la causa de la no conformidad.

10.1 No Conformidad y Acción Correctiva - Guía

Tipos

4. Llevar a cabo un análisis de las consecuencias potenciales sobre el SGSI.
5. Determinar las acciones necesarias para corregir la causa, evaluando si son proporcionales a las consecuencias y al impacto de la no conformidad.
6. Planificar las acciones correctivas dando prioridad, si es posible, a las áreas con mayor probabilidad de recurrencia y a las consecuencias más significativas de la no conformidad.
7. Implementar las acciones correctivas de acuerdo con el plan.
8. Hacer una valoración de las acciones correctivas para determinar si han manejado realmente la causa de la no conformidad y si se ha evitado que ocurran no conformidades relacionadas.

10.2 Mejora Continua –Requisito

La organización mejora continuamente la idoneidad, adecuación y eficacia del SGSI.

10.2 Mejora Continua – Explicación

Las organizaciones y sus contextos nunca son estáticos, además, los riesgos para los sistemas de información y las formas en que pueden verse comprometidos están evolucionando rápidamente. Por último, ningún SGSI es perfecto; siempre hay una forma en la que se puede mejorar, incluso si la organización y su contexto no están cambiando.

Como ejemplo de mejoras no vinculadas con no conformidades o riesgos, la evaluación de un elemento del SGSI (en términos de idoneidad, adecuación y eficacia) puede demostrar que el SGSI excede los requisitos o carece de eficiencia. Si es así, entonces puede haber una oportunidad de mejorar el SGSI.

Un enfoque sistemático que utilice la mejora continua conducirá a un SGSI más eficaz, que mejorará la seguridad de la información de la organización. La gestión de la seguridad de la información lidera las actividades operativas de la organización para evitar ser demasiado reactiva, es decir, que la mayoría de los recursos se utilizan para encontrar problemas y abordarlos. El SGSI trabaja sistemáticamente a través de la mejora continua para que la organización pueda tener un enfoque más proactivo.

10.2 Mejora Continua - Explicación

La dirección puede establecer objetivos para la mejora continua, p.e. a través de mediciones de efectividad, costo o madurez del proceso.

Como consecuencia, la organización trata su SGSI como una parte viva, en evolución y de aprendizaje del negocio.

Para que el SGSI se mantenga al día con los cambios, se evalúa periódicamente con respecto a su idoneidad para el propósito, efectividad y alineación con los objetivos de la organización.

No se debe tomar nada por sentado, y nada debe considerarse "prohibido" simplemente porque era lo suficientemente bueno en ese momento que fue implementado.

10.2 Mejora Continua - Guía

La mejora continua del SGSI debería implicar que el SGSI en sí y todos sus elementos sean evaluados considerando cuestiones internas y externas (4.1), requisitos de las partes interesadas (4.2) y resultados de evaluación del desempeño (Cláusula 9). La evaluación debe incluir un análisis de:

a) idoneidad del SGSI, considerando si las cuestiones externas e internas, requisitos de partes interesadas, objetivos de seguridad de la información establecidos y seguridad de la información identificada.

b) adecuación del SGSI, considerando si los procesos del SGSI y los controles de seguridad de la información son compatibles con los propósitos, actividades y procesos generales de la organización; y

c) eficacia del SGSI, considerando si se logran los resultados previstos del SGSI, se cumplen los requisitos de las partes interesadas, se gestionan los riesgos de seguridad de la información para cumplir los objetivos de seguridad de la información, se gestionan las no conformidades, mientras que los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI son acorde con esos resultados.

10.2 Mejora Continua - Guía

La evaluación también puede incluir un análisis de la eficiencia del SGSI y sus elementos, considerando si el uso de los recursos es adecuado, si existe el riesgo de que la falta de eficiencia pueda conducir a la pérdida de eficacia o si existen oportunidades para aumentar la eficiencia.

También se pueden identificar oportunidades de mejora al gestionar las no conformidades y las medidas correctivas.

Una vez identificadas las oportunidades de mejora, la organización debería, según 6.1.1:

d) evaluarlos para establecer si vale la pena seguirlos;

e) determinar los cambios al SGSI y sus elementos para lograr la mejora;

f) planificar e implementar las acciones para abordar las oportunidades asegurando que se obtengan los beneficios y no se produzcan no conformidades; y

g) evaluar la eficacia de las acciones.

Estas acciones deben considerarse como un subconjunto de acciones para abordar los riesgos y oportunidades descritos en 6.1.1.

¡Síguenos, ponte en contacto!

www.certiprof.com