certiprof®

ISO 27001:
INTERNAL AUDITOR /LEAD AUDITOR

PROFESSIONAL CERTIFICATION

ISO27001IA-LA™ Versión 072023

ISO 27001
INTERNAL AUDITOR/ LEAD AUDITOR
I27001 IA/LA

ISO27001IA-LA™ Versión 072023

¿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 **ATPs (Authorized TrIAning Partners.)**
- **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

Digital badges issued by

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**

itcc
IT CERTIFICATION COUNCIL

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:**

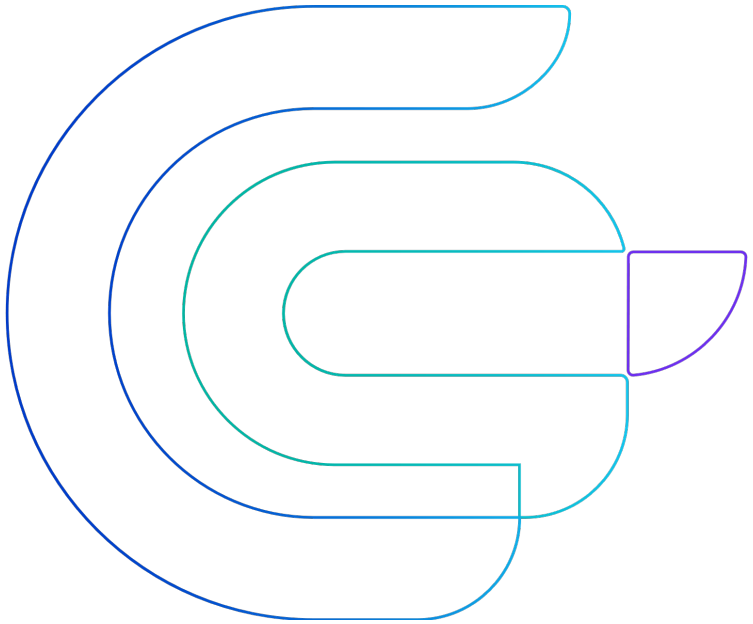
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿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

Earn this Badge

Certified ISO 27001 Internal Auditor - I27001IA

Issued by Certiprof

Earners of the ISO/IEC 27001 Internal Auditor have demonstrated a general knowledge of the standard and general concepts to develop an audit in compliance with ISO 27001 and how to evaluate the effectiveness of corrective actions applied to maintain and continuously improve an information security management system (ISMS)

Learn more

Certification $ Paid

Skills

Auditing | Continual Improvement | Customer Confidence | Data Protection

https://www.credly.com/org/certiprof/badge/certified-iso-27001-internal-auditor-i27001ia.1

Insignia

Earn this Badge

Certified ISO 27001 Lead Auditor - I27001LA™

Issued by Certiprof

Earners of the ISO/IEC 27001 Lead Auditor have demonstrated an understanding of the standard and the general concepts and requirements of ISO/IEC 27001. They have developed skills to perform the audit process and know the responsibilities of being a lead auditor and understand how to develop an ISMS.

Learn more

Certification | Paid

Skills

Compliance | Continual Improvement | Customer Confidence | Data Protection | Frameworks | Information Management & Analysis | ISMS | ISO27001 Certification | Risk Management

https://www.credly.com/org/certiprof/badge/certified-iso-27001-lead-auditor-i27001la.1

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

Objetivos

- Alcance, propósito, términos y definiciones claves de la norma ISO/IEC 27001 y cómo puede ser utilizada
- Requisitos de definición del alcance y aplicabilidad

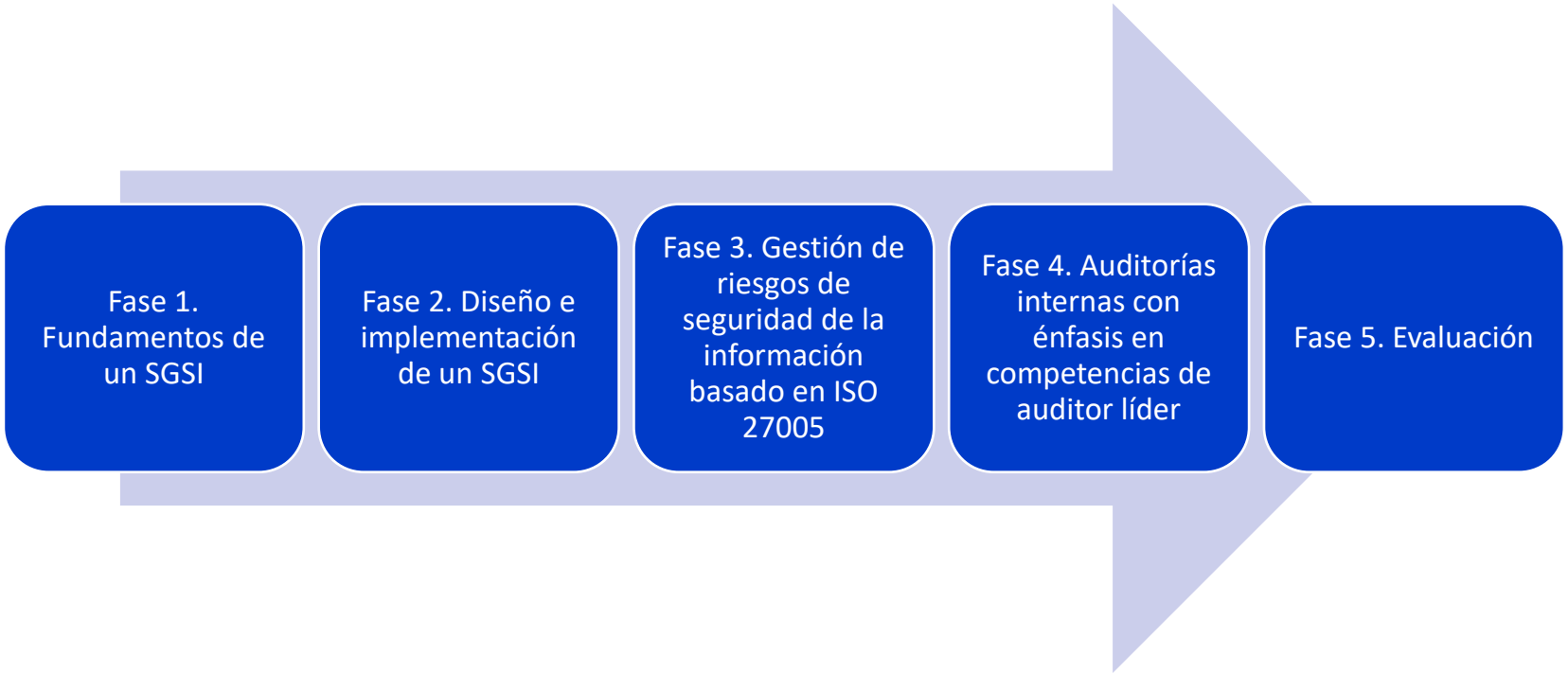
COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#ISO27001 IA-LA #certiprof

certiprof®

Agenda

Agenda


Fase 1. Fundamentos de un SGSI
Fase 2. Diseño e implementación de un SGSI
Fase 3. Gestión de riesgos de seguridad de la información basado en ISO 27005
Fase 4. Auditorías internas con énfasis en competencias de auditor líder
Fase 5. Evaluación

Fase 1. Fundamentos de un SGSI

Fundamentos de la Norma ISO 27001

- Introducción a la Norma
- Términos y definiciones
- Entendimiento de numerales de la Norma.
- Identificación de requisitos
- Qué son los objetivos de control
- Conclusiones y preguntas de apoyo

Módulo de Auditor ISO 19011

- Conceptos claves de auditoría
- Proceso de auditoría
- Componentes de la auditoría
- Preparación general para rol de auditor
- Conclusiones y preguntas de apoyo

**La agenda es una recomendación general, cada entrenador puede desarrollar el material bajo su experiencia.*

1. Introducción y Antecedentes

Introducción

- ISO/IEC 27001
- Historia de la Norma
- Estado actual
- Definiciones

Introducción

La ISO 27001:2022 es la norma internacional mas implementada y aceptada en términos de la Seguridad de la información, ciberseguridad y protección de la privacidad, porque:

- Ha sido diseñada para "*proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información*"
- *Puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con sus propios requisitos de seguridad de la información*"
- Incluye *requisitos para la valoración y tratamiento de los riesgos en la seguridad de la información*
- *Genera competitividad a la Organización, pues establece las mejores prácticas en* Seguridad de la información, ciberseguridad y protección de la privacidad *con reconocimiento internacional*
- *Se adecua a las necesidades de la organización, permitiendo certificar los procesos que se definan en el alcance del SGSI con posibilidad de ampliación en caso necesario*
- *Los requisitos establecidos en esta Norma Internacional son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza*"
- Genera capacidad de cumplimiento legal

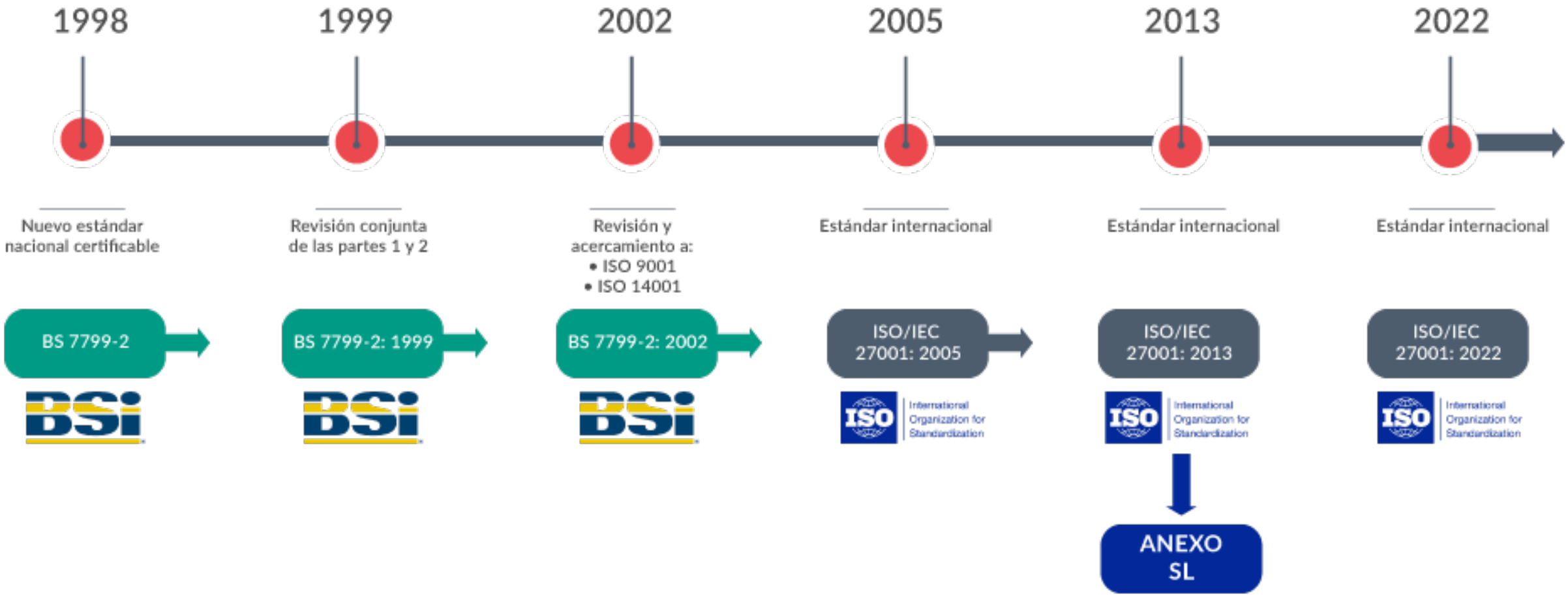
SGSI

Definición 2,34 de ISO 27000 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

Es parte del sistema de gestión global, basada en un enfoque hacia los riesgos de un negocio, para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Incluye estructura organizacional, políticas, planes, responsabilidades, procedimientos, procesos y recursos.

Historia de la Norma



ISO/IEC 27001:2022 Estructura

La Norma ISO/IEC cambió de nombre y se denomina en la versión vigente “Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos”.

La norma tiene una estructura de alto nivel, títulos de subcapítulos idénticos, texto idéntico, términos comunes, y definiciones básicas proporcionadas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO Consolidado por lo que mantiene compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.

La norma se compone de cláusulas del 4 al 10 que son requisitos obligatorios y el Anexo A que hace referencia a 93 los controles de seguridad de la información.

Los 93 controles están agrupados en 4 tipos de controles: Controles organizacionales, Controles de personal, Controles físicos y Controles tecnológicos.

Estructura de ISO/IEC 27001

0.Introducción
1.Alcance
2.Referencias normativas
3.Términos y definiciones

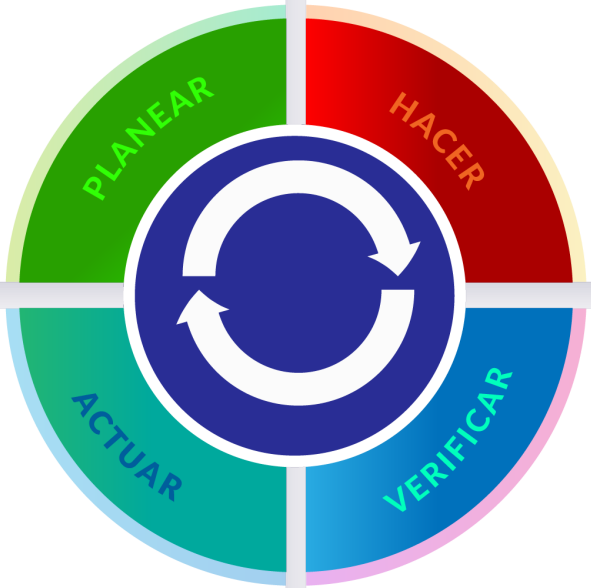
4. Contexto de la organización
5.Liderazgo
6.Planificación
7.Soporte (Apoyo)
8.Operación
9.Evaluación del desempeño
10.Mejora

Estructura de ISO/IEC 27001

Ciclo Deming PHVA Y SGSI

4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte

8. Operación



10. Mejora

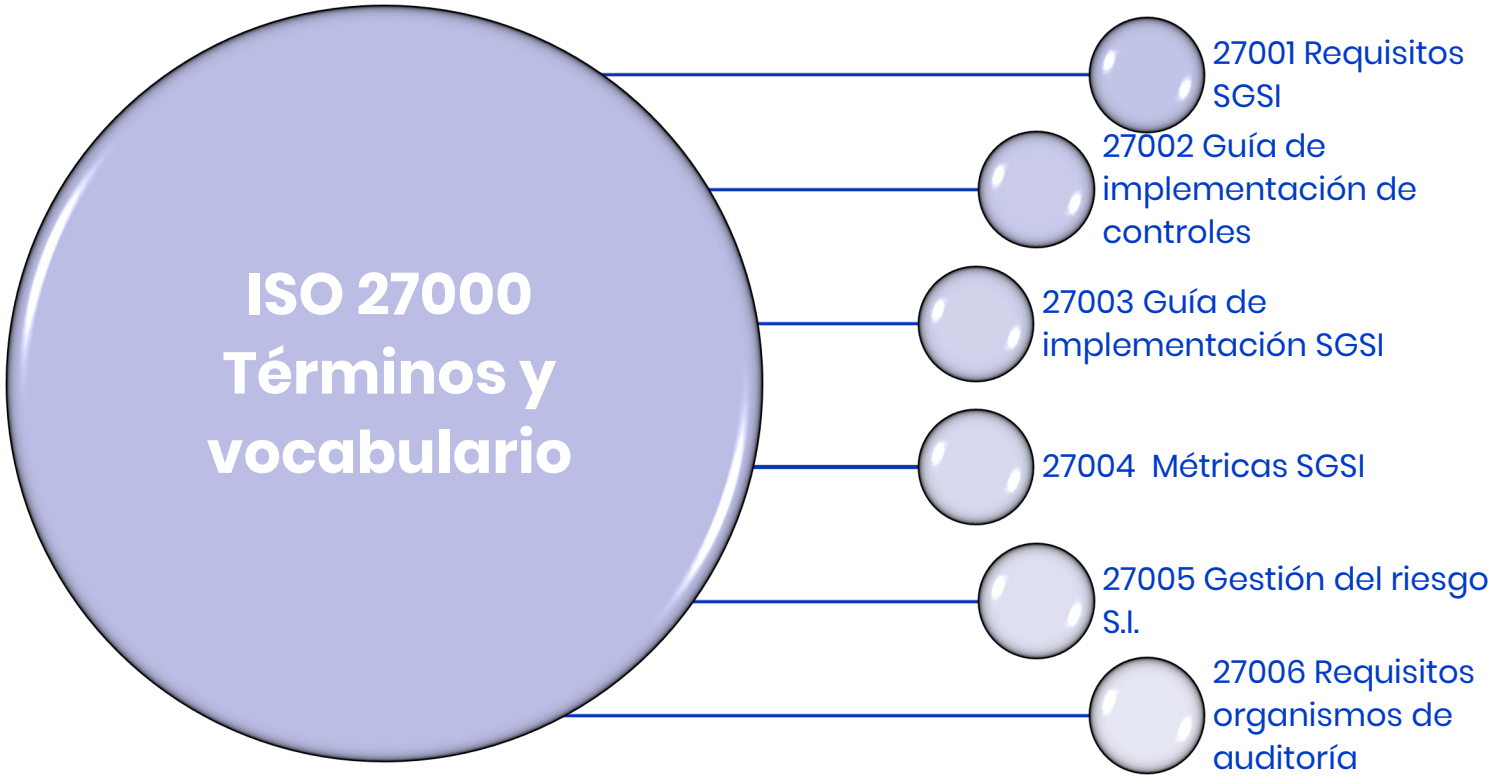
9. Evaluación de desempeño

ISO 27000 Familia de Normas

La familia de normas de SGSI cuenta con normas para:

a) Definir los requisitos para un SGSI y para los organismos que certifiquen tales sistemas
b) Abordar la evaluación de la conformidad para el SGSI
c) Proporcionar apoyo directo, orientación detallada y/o interpretación para el proceso general a establecer, implementar, mantener y mejorar un SGSI
d) Abordar directrices sectoriales específicas para el SGSI

ISO 27000 Familia de Normas



2. Conceptos Claves

¿Qué es un SGSI?

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 y la ISO 31000 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.

Información y Principios Generales

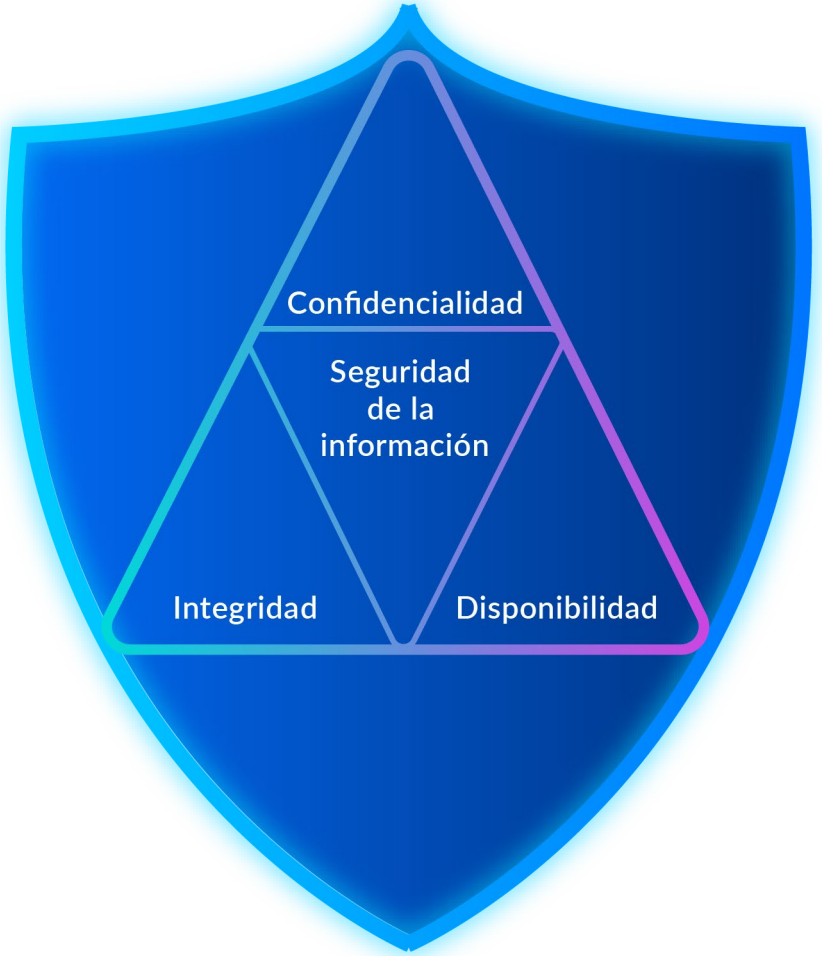
Contribución a la Organización de un **SGSI**:

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

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



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, monitorizados, 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.

El Sistema de Gestión de Seguridad de la Información

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

Factores Críticos de Éxito de una 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)

Factores Críticos de Éxito de una 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.

Beneficios de la Familia de Normas 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

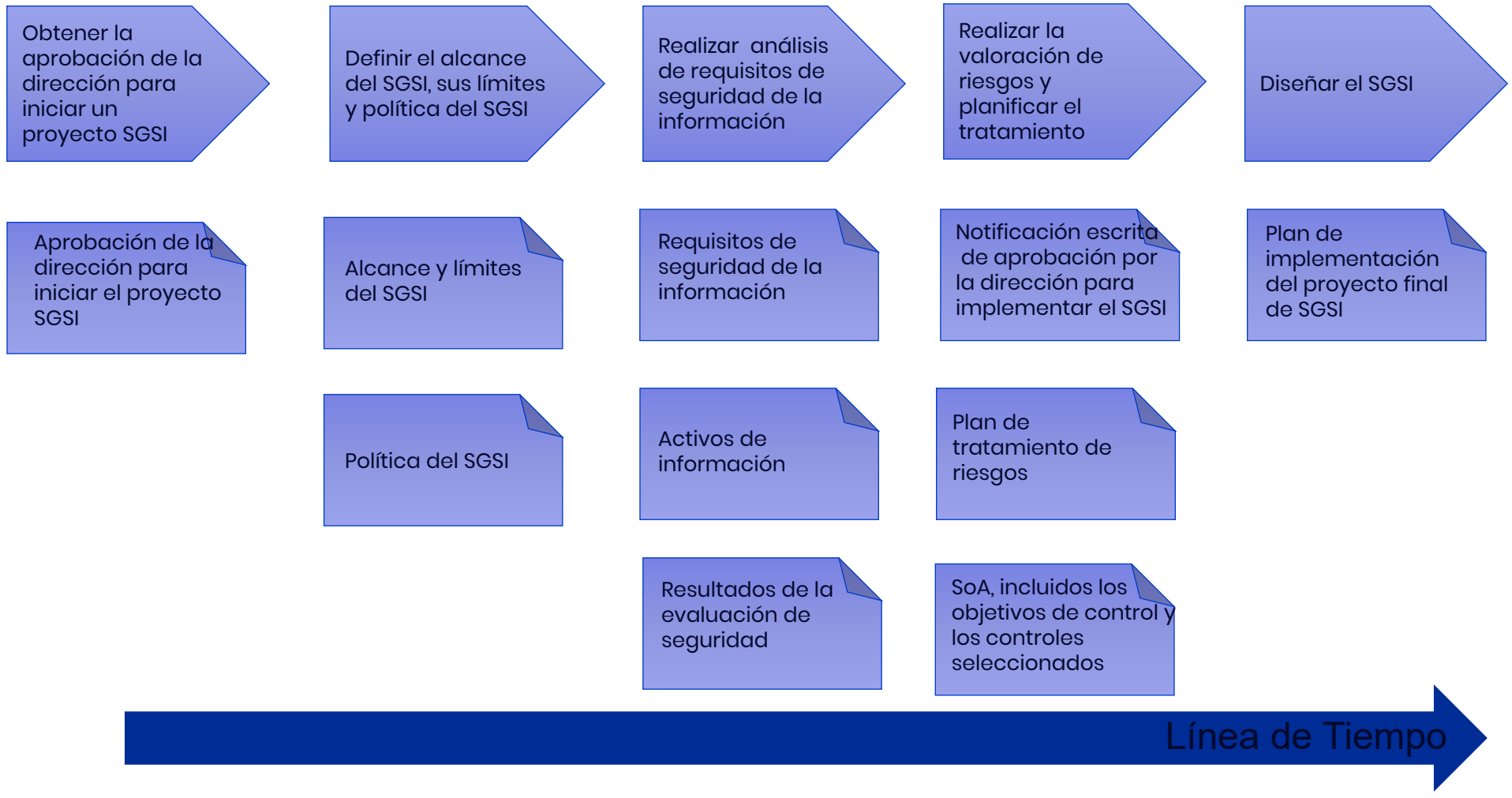
Diseño e Implementación de un SGSI

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

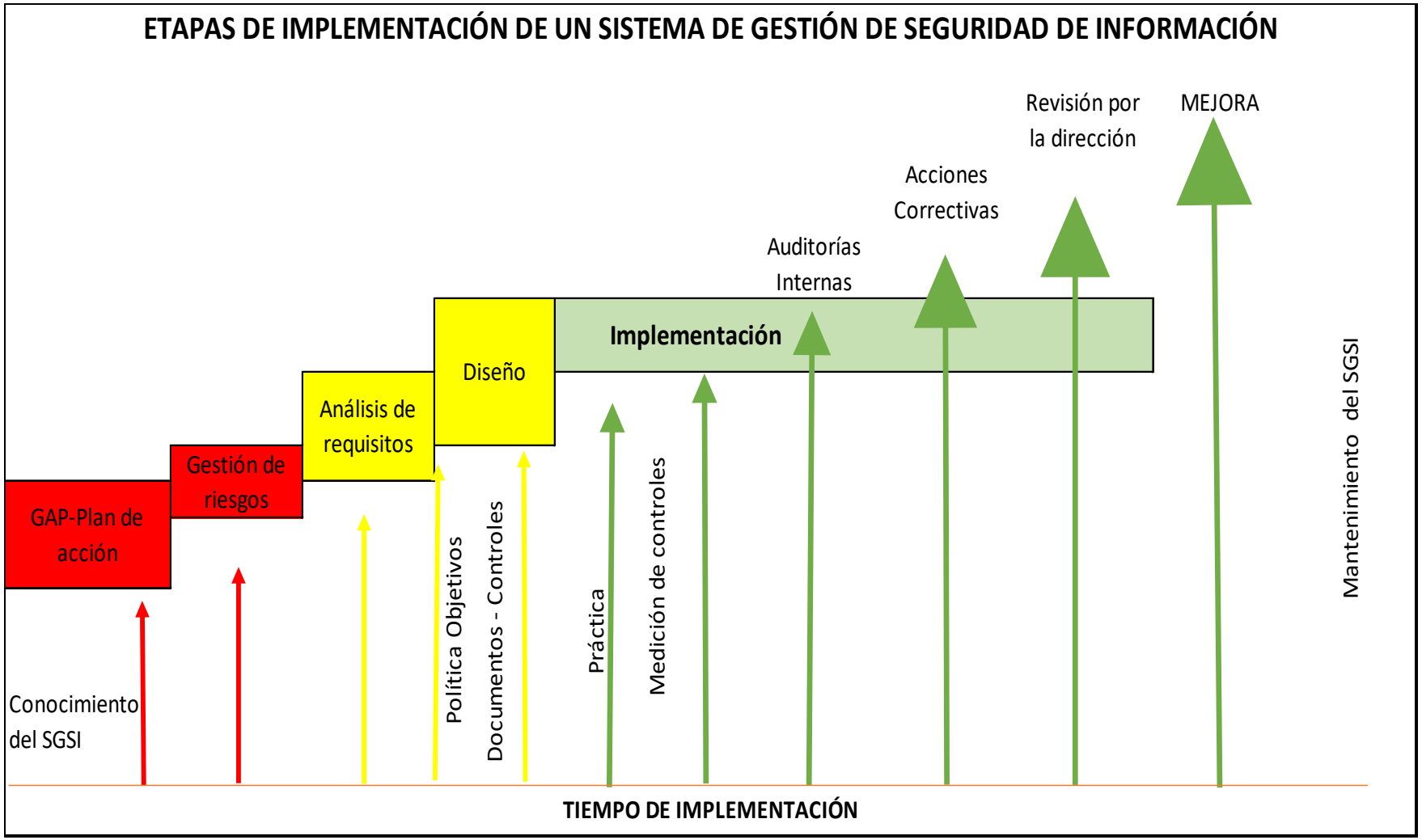
	ACTIVIDADES
1	IDENTIFICAR LÓGICAMENTE FASES DEL PROYECTO DE IMPLEMENTACIÓN DE UN SGSI SEGÚN ISO/IEC 27003
2	IDENTIFICAR, ANALIZAR, ESTABLECER E IMPLEMENTAR LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN.
3	DESARROLLAR LOS CONTROLES PROPUESTOS EN EL ANEXO A. OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA.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

NOTA: El auditor valida que estos ciclos se han cumplido con el fin de generar confianza que se han desarrollado las actividades necesarias de implementación. Existe la GUIA DE IMPLEMENTACIÓN DE UN SGSI (ISO/IEC 27003). La siguiente es la presentación de las fases del diseño e implementación:

Fases de Diseño del SGSI



Etapas de Implementación de un SGSI



3. Términos y Definiciones

(Ver complemento No. 1 Glosario ISO27001)

4. Contexto de la Organización

4.1 Comprensión de la Organización y de su Contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad de lograr el(los) resultado(s) previstos de su sistema de gestión de seguridad de la información.

NOTA: La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno

de la organización considerado en el subcapítulo 5.4.1 de ISO 31000:2018

4.1 Comprensión de la Organización y de su Contexto

- **Contexto Externo:** Es el entorno externo en el que la organización busca alcanzar sus objetivos
- **Contexto Interno:** Es el entorno interno, en el que la organización busca alcanzar sus objetivos

ENTORNO	PERSPECTIVA	TIPO
ENTORNO ECONÓMICO	Situación financera de la empresa	Interno
	Rentabilidad	Interno
	Participación de la competencia en el mercado	Externo
	Incentivos del gobierno para reactivar la economía	Externo
	La pandemia COVID 19 afectando ventas e ingresos	Externo
ENTORNO SOCIAL	Planes de formación	Interno
	Ambiente laboral	Interno
	Salario emocional	Interno
	Productividad de los clientes	Externo
ENTORNO TECNOLÓGICO	Trabajo en casa con plataformas colaborativas	Externo
	Licenciamiento de software	Interno
	Ataques cibernéticos	Externo
	Pruebas (testing)	Interno
	Servicio al cliente y atención de requerimientos (Soporte)	Interno
ENTORNO LEGAL	Legislación y cambios aplicables a la empresa	Externo
	Conocimiento de la legislación	Interno
	Aplicación normativa a procesos productivos y administrativos de la empresa	Interno
	Acuerdos de servicios con los clientes	Interno
ENTORNO AMBIENTAL	Ubicación de activos de informacion y su exposición	Interno
	Desastres naturales (incendios, inundaciones, terremotos)	Externo
ENTORNO POLITICO	Circunstacias de cambios en orientación de la Empresa	Interno
	Marchas, protestas, sindicatos	Externo

Taller 25 minutos

Determinar el Contexto de la Organización haciendo uso de una matriz de análisis FODA

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La organización debe determinar:

a) Las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información.

b) los requisitos pertinentes de estas partes interesadas.

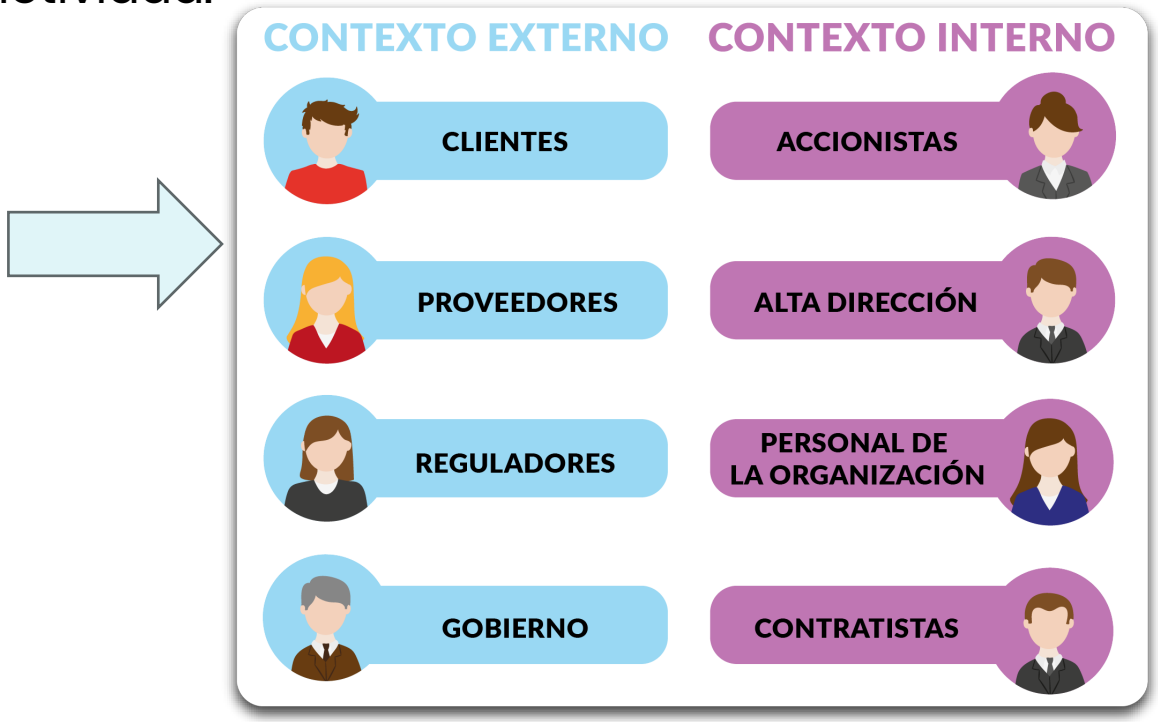
c) cuáles de estos requisitos se abordarán a través del Sistema de Gestión de Seguridad de la Información.

NOTA: Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, así como obligaciones contractuales.

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

Parte Interesada es una persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

Algunos ejemplos de partes interesadas



Prioridades de la Organización Para un SGSI

Entradas

- Objetivos estratégicos de la organización
- Panorama general de los SG actuales
- Lista de requisitos legales, reglamentarios y contractuales de S.I.

Los objetivos para implementar SGSI:

- Gestión del riesgo: Cómo el SGSI generará una mejor gestión del riesgo
- Eficiencia: En los procesos
- Ventaja competitiva: Crear V.C.

PRIORIDADES Y REQUISITOS DE S.I. A PARTIR DE LOS SIGUIENTES FACTORES:

- Áreas críticas de la organización y del negocio
- Información critica
- Normativas que exigen medidas de Seguridad de la Información.
- Acuerdos contractuales relacionados con la Seguridad de la Información
- Requisitos de la industria especifiquen controles o medidas particulares de Seguridad de la Información
- Amenazas del entorno
- Impulsores competitivos
- Requisitos de la continuidad del negocio

Salidas

- Resumen de los objetivos, las prioridades de la Seguridad de la Información. y los requisitos organizacionales para un SGSI
- Una lista de requisitos reglamentarios, contractuales y de industria, relacionados con la Seguridad de la Información de la Organización.
- Un esquema de las características del negocio, la Organización, activos y tecnología.

4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

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

Cuando se determina este alcance, la organización debe considerar:

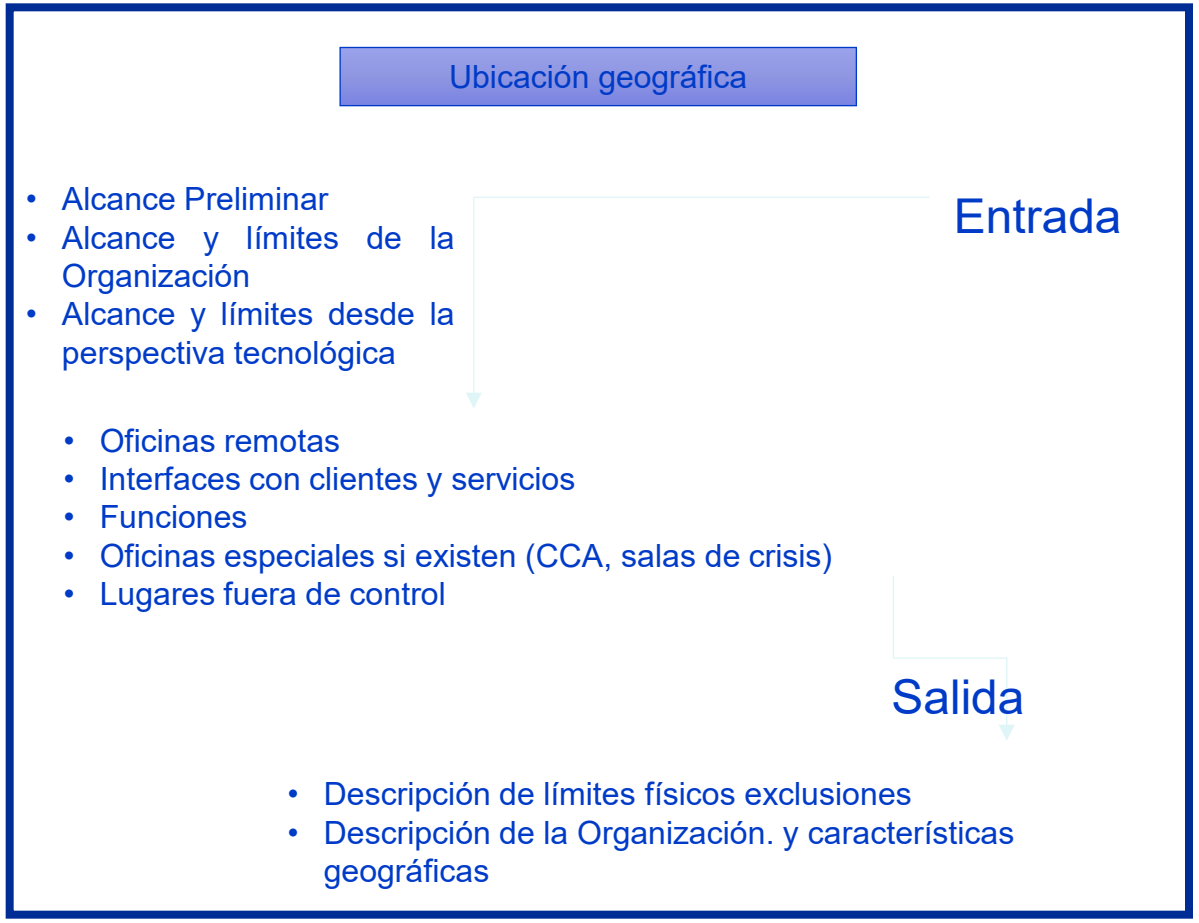
a) Las cuestiones externas e internas referidas en el apartado **4.1**
b) Los requisitos referidos en el apartado **4.2**
c) Las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones

El alcance debe estar disponible como información documentada.

4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

Un documento de definición de alcance podría considerar lo siguiente:

- Características de la organización
- Procesos de la organización
- Funciones y responsabilidades
- Activos de información
- Ubicación geográfica
- Alcance y límites desde la perspectiva organizacional
- Alcance y límites desde la perspectiva tecnológica



4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

Alcance y límites desde la perspectiva tecnológica

- Alcance Preliminar
- Alcance y límites de la Organización

Entrada

- Infraestructura
- Software
- Hardware
- Roles y responsabilidades

- Entorno socio-cultural
- Aspectos Legales
- Limitaciones técnicas

Salida

Alcance y límites desde la perspectiva organizacional

- Alcance Preliminar
- Prioridades de la Organización

Entrada

- Procesos, ubicaciones físicas, Sistemas de Información
- Activos de Información y Riesgos asociados
- Identificar áreas de responsabilidades que se superponen
- Identificar todo el personal afectado por el SGSI.

Salida

- Descripción de los límites de la Organización. Para el SGSI y exclusiones
- Funciones y estructuras incluidas en el alcance
- Información intercambiada en el alcance y en los límites
- Los procesos y las responsabilidades de los A.I. incluidos

4.4 Sistema de Gestión de la Seguridad de la Información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta norma internacional.

Taller 25 minutos

Definir el alcance del SGSI

5. Liderazgo

5.1 Liderazgo y Compromiso

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

a) Asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización.

b) Asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización.

c) Asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

5.1 Liderazgo y Compromiso

d) Comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.
e) Asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).
f) Dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información.
g) Promoviendo la mejora continua.
h) Apoyando a otros roles de gestión pertinentes para demostrar su liderazgo en lo que respecta a sus áreas de responsabilidad.

NOTA: La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.1 Liderazgo y Compromiso

El compromiso de la Alta Dirección puede demostrarse por ejemplo por:

- Estableciendo, Aprobando y Apoyando el cumplimiento una Política de Seguridad de la información
- Aprobar y Asegurar los recursos necesarios para el SGSI
- Asegurando que el SGSI tiene definidos los roles, las responsabilidades y las autoridades
- Comunicando la importancia de la Seguridad de la Información
- Motivando a los colaboradores para contribuir a la eficacia del SGSI
- Fortaleciendo la rendición de cuentas por resultados de gestión de seguridad de la información
- Estableciendo las condiciones adecuadas para el involucramiento de los colaboradores en el logro de los objetivos de seguridad de información de la organización

5.2 Política

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

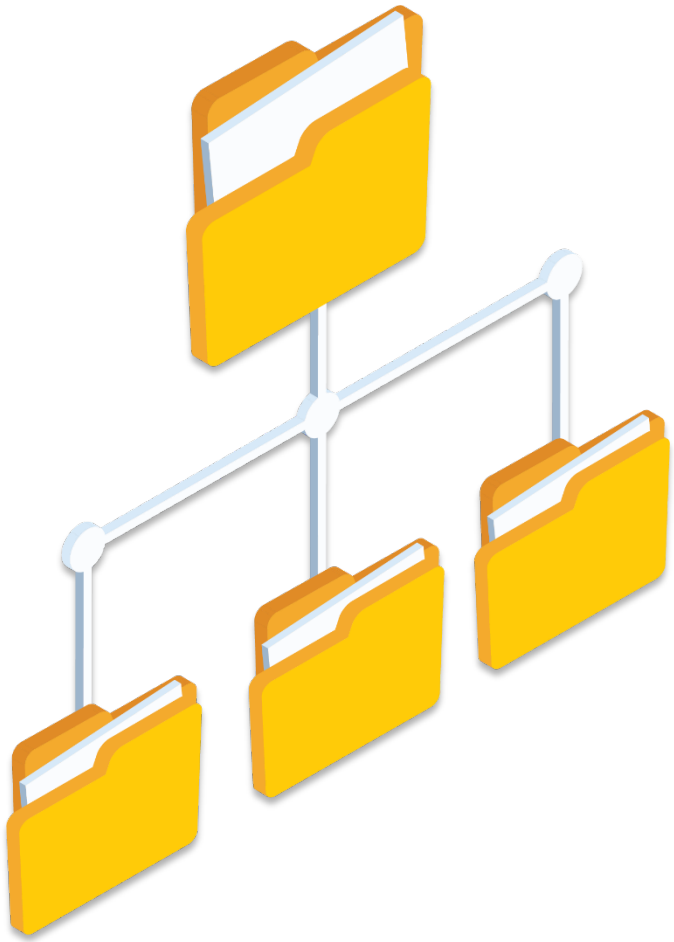
a) Sea adecuada al propósito de la organización

b) Incluya objetivos de seguridad de la información (véase **6.2**) o proporcione un marco de referencia para el establecimiento de los objetivos de seguridad de la información

c) Incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información.

d) Incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información

5.2 Política



La política de seguridad de la información debe:

e) Estar disponible como información documentada.

f) Comunicarse dentro de la organización.

g) Estar disponible para las partes interesadas, según sea apropiado.

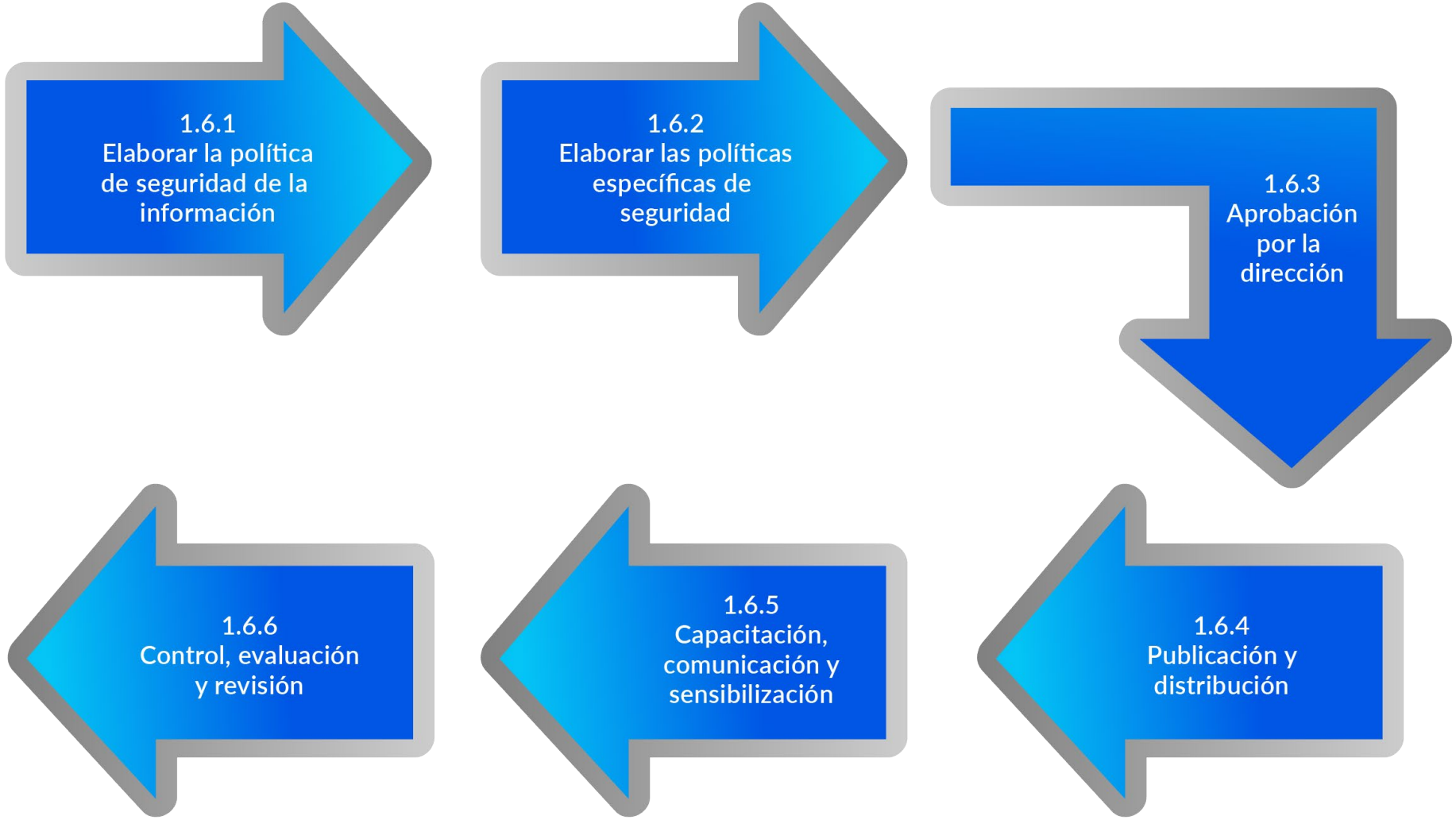
5.2 Política

Algunos métodos de comunicación interna de la Política de Seguridad de la Información pueden ser los siguientes:

- Inducción y entrenamiento mediante charlas
- Envío por correo electrónico
- Entrega de manera personal
- Publicación en tablones de anuncios (Declaración de Política de Seguridad de la Información)
- Publicación en la Intranet corporativa

No obstante, estos métodos pueden usarse de manera individual o de forma combinada como parte de un Programa permanente de Sensibilización en Seguridad de la Información y se debe asegurar que los colaboradores comprendan y entiendan la Política de Seguridad de la Información; estos resultados pueden medirse mediante la realización de evaluaciones periódicas y así generar registros con los resultados obtenidos y determinar mejoras.

5.2 Política


1.6.1
Elaborar la política de seguridad de la información
1.6.2
Elaborar las políticas específicas de seguridad
1.6.3
Aprobación por la dirección
1.6.4
Publicación y distribución
1.6.5
Capacitación, comunicación y sensibilización
1.6.6
Control, evaluación y revisión

5.3 Roles, Responsabilidades y Autoridades en la Organización

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

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma internacional

b) Informar a la alta dirección sobre el comportamiento del sistema de gestión de la seguridad de la información

NOTA: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.

5.3 Roles, Responsabilidades y Autoridades en la Organización

En esta fase de ha de definir claramente los Roles, Responsabilidades y Autoridades sobre Seguridad de la Información para ello es necesario designar al responsable de seguridad de la Información , establecer las autoridades que pueden ser mediante la designación de un Comité SGSI.

Las buenas prácticas nos indican que este Comité SGSI puede estar conformado por representantes las áreas de la relevantes de la organización como por ejemplo Alta Dirección, Administración y Finanzas, Recursos Humanos, Tecnología de Información y Legal.

Asimismo, se deben establecer las responsabilidades para el Oficial de Seguridad de la Información, el Comité SGSI (de ser el caso) y los Colaboradores de la Organización.

Es importante que tener en cuenta que el responsable de Seguridad de la Información no debe depender jerárquicamente del área de TI porque se debe tener independencia y permitir adecuadamente se cumpla con la segregación de funciones.

6. Planificación

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1.1 Consideraciones Generales

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones referidas en el subcapítulo 4.1 y los requisitos referidos en el subcapítulo 4.2 y determinar los riesgos y oportunidades que necesitan ser abordados para:

a) Asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos.
b) Prevenir o reducir efectos no deseados.
c) Lograr la mejora continua.

6.1 Acciones para Tratar los Riesgos y Oportunidades

La organización debe planificar:

d) Las acciones que aborden estos riesgos y oportunidad

e) La forma de:

1. Integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información.
2. Evaluar la eficacia de estas acciones.

CONTEXTO (Cláusula 4.1)	PARTES INTERESADAS (Cláusula 4.2)	RIESGOS Y OPORTUNIDADES (Cláusula 6.1)
Regulatorio	Recursos humanos (Contratos)	No se cumplen los requisitos legales

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1.2 Evaluación del riesgo de seguridad de la información

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

a) Establezca y mantenga criterios sobre riesgos de seguridad de la información incluyendo:
   1. Los criterios de aceptación de los riesgos
   2. Los criterios para llevar a cabo las evaluaciones de los riesgos de seguridad de la información.

b) Asegure que las sucesivas evaluaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables.

c) Identifique los riesgos de seguridad de la información:
   1. Llevando a cabo el proceso de evaluación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información
   2. Identificando a los propietarios de los riesgos

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1 Acciones para Tratar los Riesgos y Oportunidades

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

Riesgo: Efecto de la incertidumbre en los objetivos.

Un efecto es una desviación de lo esperado; puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

Positivo: Ganancia Potencial / **Negativo:** Suceso perjudicial.

Los objetivos pueden tener diferentes aspectos y categorías, y pueden aplicarse a diferentes niveles.

El riesgo se expresa generalmente en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y su probabilidad.

6.1 Acciones para Tratar los Riesgos y Oportunidades

Nivel de riesgo: Magnitud de un riesgo expresada en términos de la combinación de las consecuencias y de su probabilidad.

Los riesgos de seguridad de la información son los asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información.

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1 Acciones para Tratar los Riesgos y Oportunidades

- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser aprovechado por una o más amenazas
- **Control:** medida que modifica el riesgo.

6.1 Acciones para Tratar los Riesgos y Oportunidades

d) Analice los riesgos de seguridad de la información:
   1. Evaluando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse.
   2. Evaluando la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1)
   3. Determinando los niveles de riesgo

e) Valore los riesgos de seguridad de la información:
   1. Comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a)
   2. Priorizando los riesgos analizados para el tratamiento de riesgos.

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

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1.3 Tratamiento de los Riesgos de Seguridad de la Información

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

a) Seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información teniendo en cuenta los resultados de la apreciación de riesgos
b) Determinar todos los controles que sean necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información

NOTA 1: Las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente.

6.1 Acciones para Tratar los Riesgos y Oportunidades

c) Comparar los controles determinados en el punto **6.1.3 b)** con los del anexo A y comprobar que no se han omitido controles necesarios

NOTA 2: El anexo A contiene una lista de posibles controles de seguridad de la información. Se indica a los usuarios de esta norma internacional que se dirijan al anexo A para asegurar que no se pasan por alto controles necesarios.

NOTA 3: Los controles de seguridad de la información del Anexo A, no son exhaustivos, por lo que pueden ser necesarios objetivos de control y controles adicionales.

6.1 Acciones para Tratar los Riesgos y Oportunidades

d) Producir una ***"Declaración de Aplicabilidad"*** que contenga:

- Los controles necesarios [véase **6.1.3 b) y c)**]
- La **justificación de las inclusiones**
- Si los controles necesarios están implementados o no
- La **justificación de las exclusiones** de cualquiera de los controles del anexo A

6.1 Acciones para Tratar los Riesgos y Oportunidades

e) Formular **un plan de tratamiento de riesgos** de seguridad de la información
f) Obtener la aprobación del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información por parte de los propietarios de los riesgos.

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

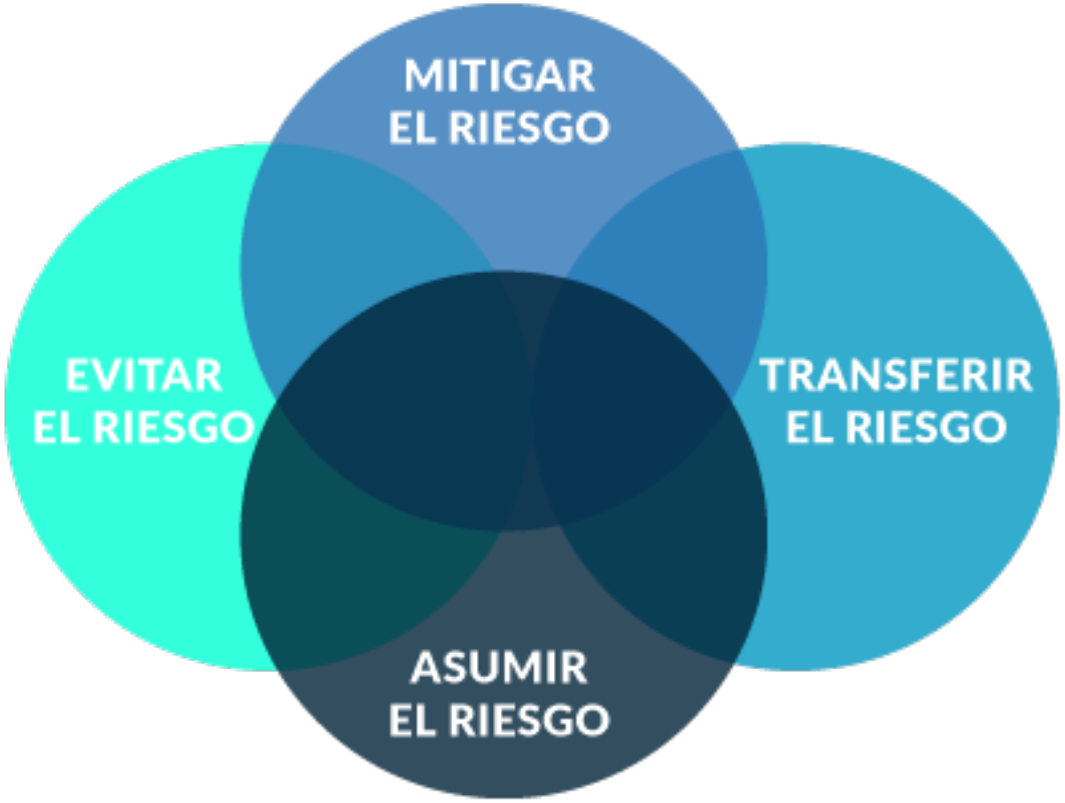
NOTA: La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en esta norma internacional se alinean con los principios y directrices genéricas definidos en la **Norma ISO 31000**.

6.1 Acciones para Tratar los Riesgos y Oportunidades

Declaración de Aplicabilidad (Statement of Applicability –SoA)

Control	Nombre del control	Descripción del control	Aplicable	Justifiación aplicablilidad /exclusión
5.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas a y reconocido por el personal pertinente y las partes interesadas pertinentes, y revisado a intervalos planificados y si se producen cambios significativos.	SI	Información documentada requerida
7.10	Medios de almacenamiento	Los medios de almacenamiento se gestionarán a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con las normas de la organización. esquema de clasificación y requisitos de manipulación.	NO	No se manejan medios de almacenamiento

6.1 Acciones para Tratar los Riesgos y Oportunidades



Estrategias:

- **Mitigar**: Implemento controles para reducir el nivel de riesgo
- **Asumir:** Se asume o retiene el riesgo en su nivel actual
- **Transferir:** Comparto el riesgo con partes externas (compra de un seguro o tercerización de servicios)
- **Evitar:** Cancelo la actividad que genera el riesgo

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 Acciones para Tratar los Riesgos y Oportunidades

Riesgo residual: riesgo remanente después del tratamiento del riesgo.

Estructura de la Norma ISO 31000 Gestión de Riesgos – Directrices

- Este documento proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto
- Este documento proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector
- Este documento puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles

6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución

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

Los objetivos de seguridad de la información deben:

a) Ser coherentes con la política de seguridad de la información.
b) Ser medibles (si es posible).
c) Tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y del tratamiento de los riesgos.
d) Ser objeto de seguimiento.
e) Ser comunicados.
f) Actualizarse según corresponda.
g) Estar disponible como información documentada.

6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución

La organización debe conservar información documentada sobre los objetivos de seguridad de la información.

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

h) Lo que se va a hacer.
i) Qué recursos serán requeridos.
j) Quién será responsable.
k) Cuando se finalizará.
l) Cómo se evaluarán los resultados.

6.2 Objetivos de Seguridad de la Información y Planificación para su Consecución

Ejemplo de un objetivo del SGSI para el Servicio de Seguridad Gestionada por un Security Operation Center (SOC).

OBJETIVO ESTRATÉGICO	OBJETIVO ESPECIFICO	DESCRIPCIÓN	INDICADOR	META	UMBRALES DE ACEPTACIÓN		MEDIOS	PERIODICIDAD	RESPONSABLE DE MEDICIÓN	RESPONSABLE DE EVALUACIÓN
Buscar la permanente satisfacción de nuestros clientes	Cumplimiento contractual	Cumplir requisitos contractuales asociados a contratos	Incumplimiento de SLA de contratos	Igual o menor que 5 %	Igual o menor que 5 %	Bueno	Reporte de incidentes del servicio	Mensual	Jefe de SOC	Oficial de seguridad de informacón
					Entre 6 % y 7%	Regular				
					Mayor o igual a 8%	Malo				

6.3 Planificación de Cambios

Cuando la organización determina la necesidad de cambios en el sistema de gestión de la seguridad de la información, los cambios deben ser llevados a cabo de manera planificada.

7. Soporte

7.1 Recursos

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

7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información

b) Asegurarse que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas.

c) Cuando sea aplicable, poner en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo

d) Conservar la información documentada apropiada, como evidencia de la competencia

NOTA: Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3 Concienciación

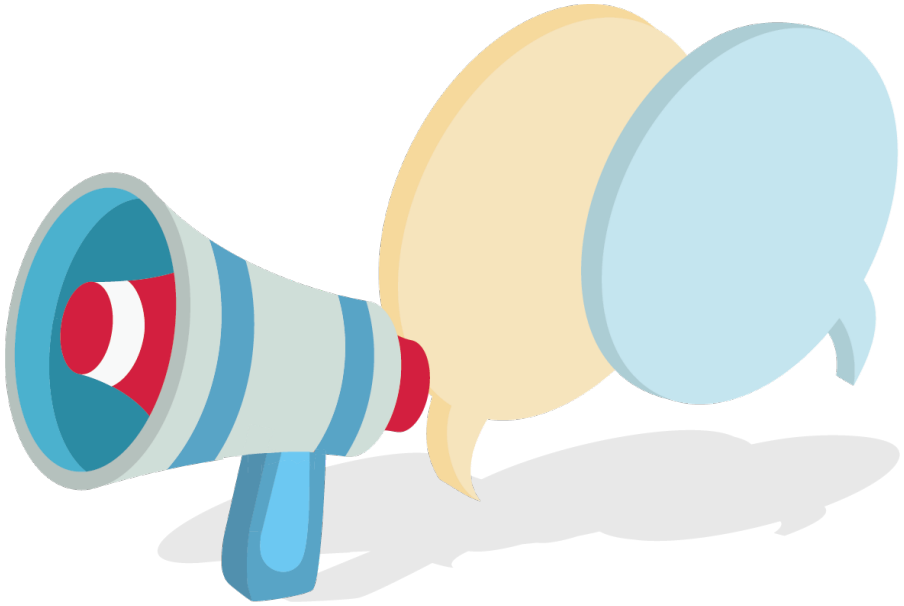
Las personas que trabajan bajo el control de la organización deben ser conscientes de:

a) La política de la seguridad de la información

b) Su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información

c) Las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información

7.4 Comunicación



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

a) sobre qué comunicar
b) cuando comunicar
c) con quién comunicarse
d) cómo comunicarse

7.5 Información Documentada

7.5.1 Consideraciones Generales

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

a) La información documentada requerida por esta norma internacional

b) La información documentada que la organización ha determinado que es necesaria para la efectividad del sistema de gestión de la seguridad de la información

NOTA: El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

1. El tamaño de la organización y a su tipo de actividades, procesos, productos y servicios
2. La complejidad de los procesos y sus interacciones
3. La competencia de las personas

7.5 Información Documentada

7.5.2 Creación y Actualización

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

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

7.5 Información Documentada

7.5.3 Control de la Información Documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma internacional se debe controlar para asegurarse que:

a) Esté disponible y preparada para su uso, dónde y cuándo se necesite

b) Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad)

7.5 Información Documentada

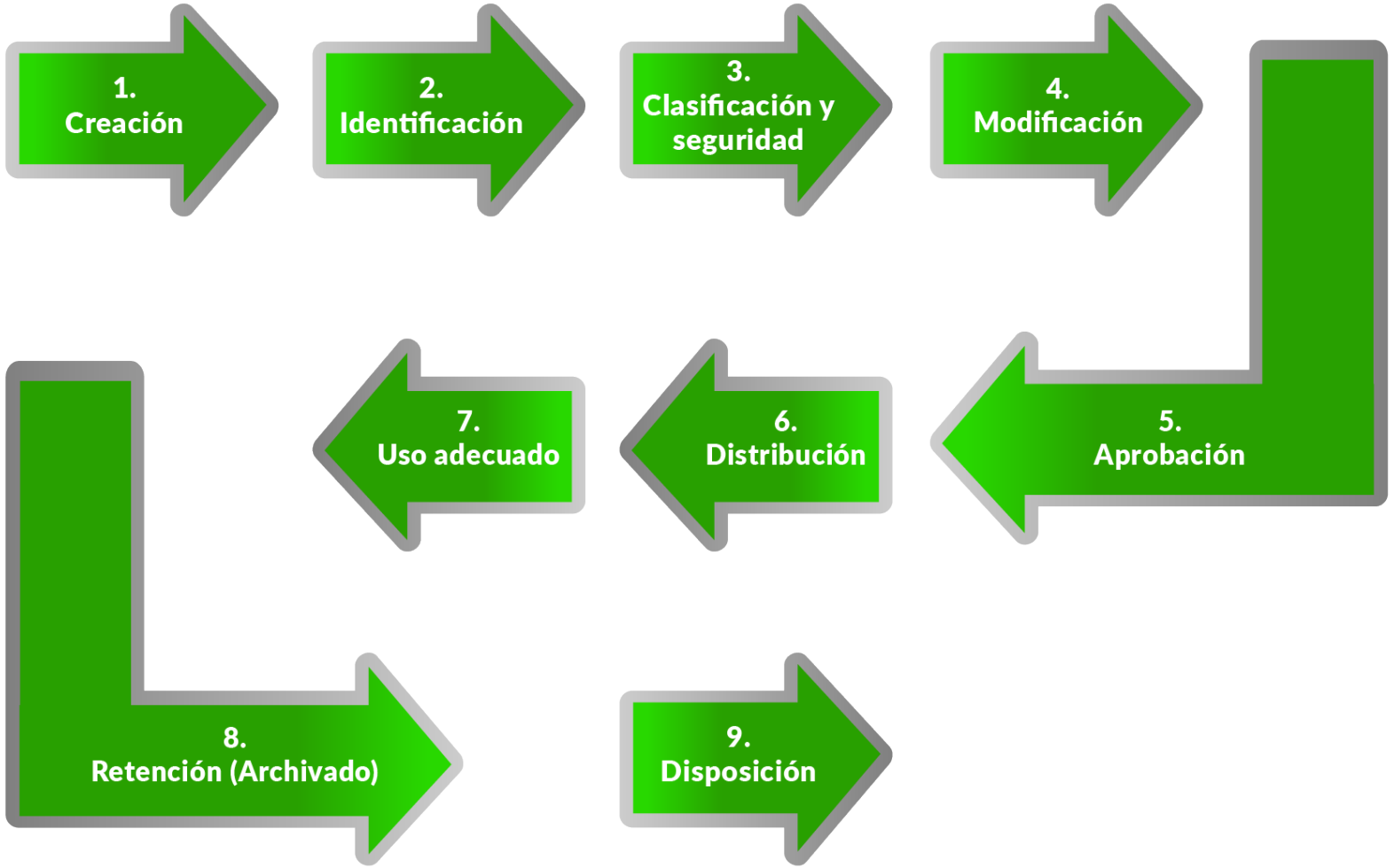
Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) Distribución, acceso, recuperación y uso
d) Almacenamiento y preservación, incluida la preservación de la legibilidad
e) Control de cambios (por ejemplo, control de versión)
f) Retención y disposición

La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, debe ser identificada según sea apropiado y controlarse.

NOTA: El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

7.5 Información Documentada



8. Operación

8.1 Planificación y Control Operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos e implementar las acciones determinadas en la Cláusula 6, mediante:

Establecer criterios para los procesos.

Implementar el control de los procesos de acuerdo con los criterios.

8.1 Planificación y Control Operacional

Se dispondrá de información documentada en la medida necesaria para tener confianza en que los
procesos se han llevado a cabo según lo previsto.

La organización debe controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurar que los procesos, productos o servicios provistos de forma externa que son pertinentes para el sistema de gestión de seguridad de la información, son controlados.

8.2 Evaluación de Riesgos de Seguridad de la Información

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

La organización debe conservar información documentada de los resultados de las apreciaciones de riesgos de seguridad de información.

TABLA 02: PROBABILIDAD DE OCURRENCIA

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias expecionales.	No se ha presentado en los últimos 3 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos una vez en los últimos 3 años.
3	Posible	El evento podría ocurrir en algún momento.	Al menos una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una vez al año.

TABLA 03: NIVEL DE IMPACTO

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Dañino	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Severo	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Crítico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

TABLA 04: MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

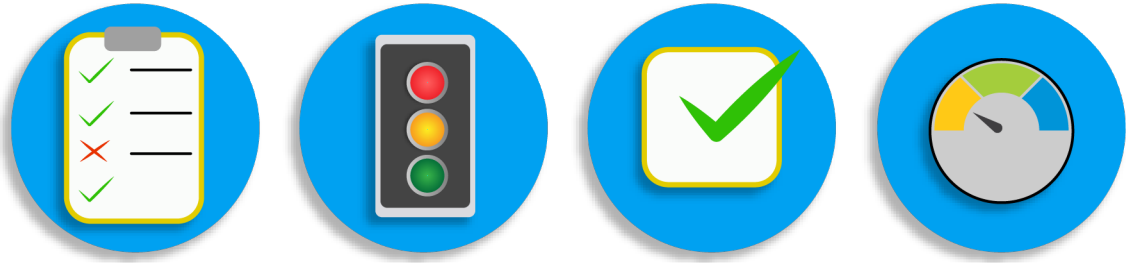
Probabilidad	Impacto: 1 Insignificante	2 Menor	3 Dañino	4 Severo	5 Crítico
1 Raro	B(1)	B(2)	M(3)	M(4)	M(5)
2 Improbable	B(2)	M(4)	M(6)	M(8)	M(10)
3 Posible	M(3)	M(6)	A(9)	A(12)	A(15)
4 Probable	M(4)	M(8)	A(12)	A(16)	E(20)
5 Casi Seguro	M(5)	M(10)	A(15)	A(20)	E(25)

B	Zona de riesgo baja.	Asumir el riesgo.
M	Zona de riesgo moderada.	Asumir el riesgo, evaluar, reducir el riesgo.
A	Zona de riesgo alta.	Reducir el riesgo, evitar, compartir o transferir.
E	Zona de riesgo extrema.	Reducir el riesgo, evitar, compartir o transferir.

8.3 Tratamiento de los Riesgos de Seguridad de la Información

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

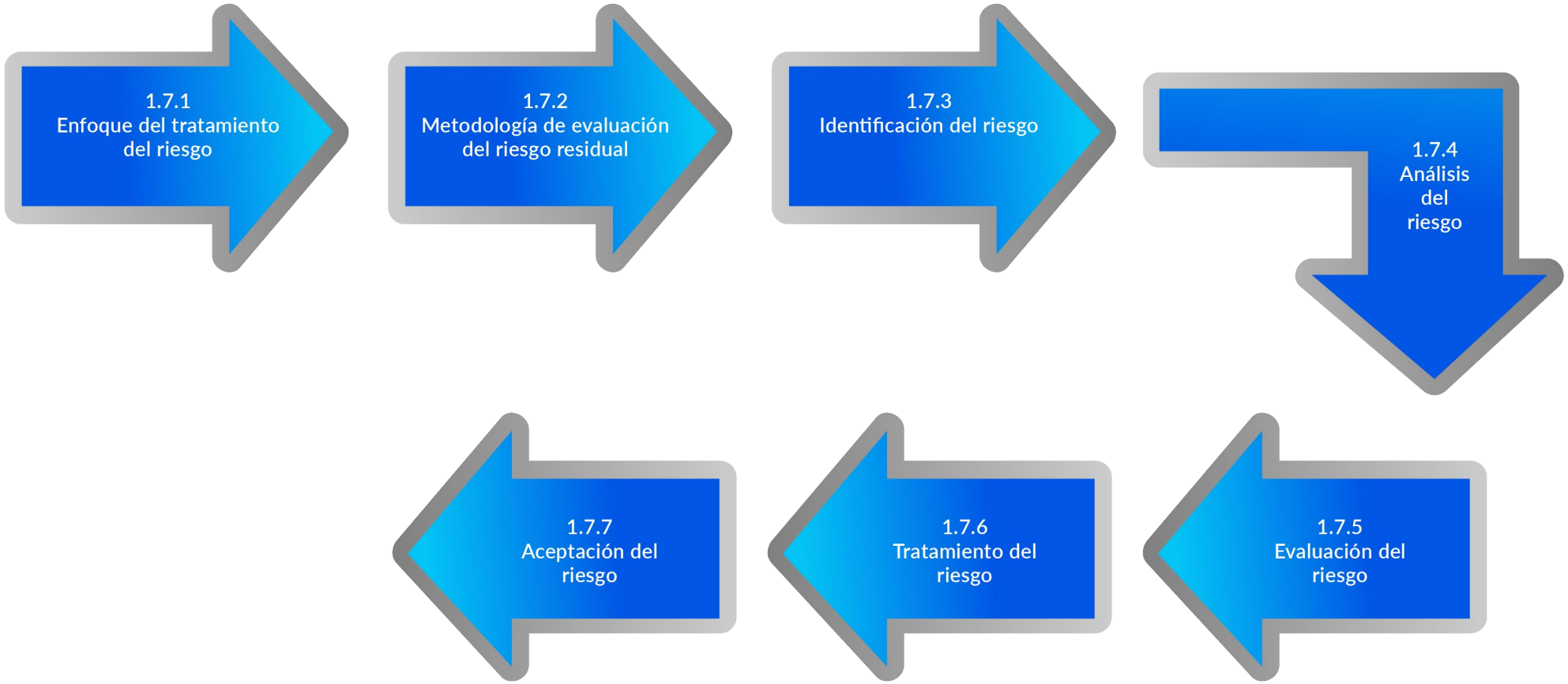
La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.



8.3 Tratamiento de los Riesgos 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

Evaluación y Tratamiento de Riesgos



9. Evaluación del Desempeño

9.1 Seguimiento, Medición, Análisis y Evaluación

La organización debe determinar:

a) A qué es necesario hacer seguimiento y qué es necesario medir, incluyendo procesos y controles de seguridad de la información

b) Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos. Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

9.1 Seguimiento, Medición, Análisis y Evaluación

c) Cuando se debe realizar el seguimiento y medición.
d) Quién debe hacer el seguimiento y la medición.
e) Cuando se deben analizar y evaluar los resultados del seguimiento y la medición.
f) Quién debe analizar y evaluar esos resultados.

La información documentada debe estar disponible como evidencia de los resultados.

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

9.1 Seguimiento, Medición, Análisis y Evaluación

9.2 Auditoría Interna

9.2.1 Generalidades

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

a) Cumple con:
1. Los requisitos propios de la organización para su sistema de gestión de la seguridad de la información.
2. Los requisitos de esta norma internacional.

b) Se implementa y mantiene de manera efectiva

9.2 Auditoría Interna

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación e informes.

Cuando se establezca el (los) programa(s) de auditoría interna, la organización debe tomar en consideración la importancia de los procesos involucrados y los resultados de auditorías previas.

9.2 Auditoría Interna

9.2.2 Programa de auditoría interna

La organización debe:
a) definir los criterios y el alcance de cada auditoría.
b) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría.
c) asegurar que los resultados de las auditorías se reporten a los gerentes pertinentes.

Información documentada debe estar disponible como evidencia de la implementación del programa de auditoría y los resultados de la auditoría.

Auditoría

- **Auditoría** se define como el proceso sistemático, independiente y documentado para obtener evidencia objetiva y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría

- **Evidencia objetiva** datos que respaldan la existencia o la verdad de algo. La evidencia objetiva se puede obtener a través de observación, medición, prueba o por otros medios. 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

- **Criterios de auditoría** conjunto de requisitos utilizados como referencia con respecto a los cuales se compara la evidencia objetiva. 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 Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, etc.

Auditoría

- **Alcance de auditoría** se refiere al alcance y límites de una auditoría. El alcance de la auditoría generalmente incluye una descripción de las ubicaciones físicas y virtuales, funciones, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto. Una ubicación virtual es cuando una organización realiza un trabajo o proporciona un servicio usando un entorno en línea que permite a las personas, independientemente de las ubicaciones físicas, ejecutar procesos

9.3 Revisión por la Dirección

9.3.1Generalidades
La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continua.

9.3.2 Entradas para la revisión por la dirección
La revisión por la dirección debe incluir consideraciones sobre:

a) El estado de las acciones desde anteriores revisiones por la dirección.
b) Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información.

9.3 Revisión por la Dirección

c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información.

d) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:

1) no conformidades y acciones correctivas;
2) resultados del seguimiento y medición;
3) resultados de auditoría;
4) cumplimiento de los objetivos de seguridad de la información

9.3 Revisión por la Dirección

e) retroalimentación de partes interesadas.

f) Los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.

g) Las oportunidades de mejora continua

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas a oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de seguridad de la información.

La información documentada debe estar disponible como evidencia de los resultados de revisiones por parte de la dirección.

9.3 Revisión por la Dirección

Las actas de Revisión por la Dirección se debe incluir estos puntos como mínimo y estar numeradas en orden correlativo.

1) Acciones de seguimiento de los acuerdos del Acta anterior de Reunión del Comité SGSI.
2) Cambios en los asuntos externos e internos que son pertinentes al SGSI.
3) Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI
4) Los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en no conformidades y acciones correctivas
5) Resultados del monitoreo y mediciones
6) Resultados de auditoría
7) Cumplimiento de los objetivos de seguridad de la información.
8) Comentarios de las partes interesadas.
9) Resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo.
10) Oportunidades para la mejora continua.

10. Mejora

10.1 Mejora continua 10.2 No conformidad y acciones correctivas

10.1. Mejora continua: La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información.

10.2. No conformidad y acciones correctivas: Cuando ocurra una no conformidad, la organización debe:

a) Reaccionar ante la no conformidad, y según sea aplicable:
   1. Llevar a cabo acciones para controlarla y corregirla
   2. Hacer frente a las consecuencias

b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante:
   1. La revisión de la no conformidad
   2. La determinación de las causas de la no conformidad
   3. La determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir

10.2 No Conformidad y Acciones Correctivas

c) Implementar cualquier acción necesaria
d) Revisar la eficacia de las acciones correctivas llevadas a cabo
e) Si es necesario, hacer cambios al sistema de gestión de la seguridad de la información

Las acciones correctivas deben ser adecuadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada, como evidencia de:
f) La naturaleza de las no conformidades y cualquier acción posterior llevada a cabo
g) Los resultados de cualquier acción correctiva

Anexo A: Normativo

(Ver Objetivos de Control I27001IA-LA)

Anexo A: Controles

REQUISITOS ISO/IEC 27001:2022

4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

ANEXO A ISO/IEC 27001:2022

- 5. Controles Organizacionales
- 6. Controles de personas
- 7. Controles físicos
- 8. Controles tecnológicos

Nota: El auditor NO solo evalúa los requisitos 4 al 10, sino también los controles del Anexo A que se explican a continuación.

Favor apoyarse del complemento No. 2.

Anexo A: Cláusulas, Objetivos y Controles

Los controles de seguridad de la información listados en Anexo A son directamente derivados desde y alineados con los listados en la Norma ISO/IEC 27002:2022 capítulos 5 a 8. y deben ser utilizados en el contexto con el punto 6.1.3. de la ISO/IEC 27001:2022.

4 GRUPOS

Controles Organizacionales
Controles de personas
Controles físicos
Controles tecnológicos

93 CONTROLES

5. Controles Organizacionales

- 5.1 Políticas de seguridad de la información.
- 5.2 Roles y responsabilidades en seguridad de la información
- 5.3 Segregación de funciones
- 5.4 Responsabilidades de gestión
- 5.5 Contacto con autoridades
- 5.6 Contacto con grupos de interés
- 5.7 Inteligencia de amenazas
- 5.8 Seguridad de la información en la gestión de proyectos
- 5.9 Inventario de información y otros activos asociados
- 5.10 Uso aceptable de información y otros activos asociados

5. Controles Organizacionales

- 5.11 Retorno de activos
- 5.12 Clasificación de la información
- 5.13 Etiquetado de información
- 5.14 Transferencia de información
- 5.15 Control de acceso
- 5.16 Gestión de identidad
- 5.17 Información de autenticación
- 5.18 Derechos de acceso
- 5.19 Seguridad de la información en la relación con proveedores
- 5.20 Abordar la seguridad de la información dentro de los acuerdos de proveedores

5. Controles Organizacionales

- 5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
- 5.22 Monitoreo, revisión y gestión del cambio en los servicios de los proveedores
- 5.23 Seguridad de la información para el uso de servicios Cloud
- 5.24 Planificación y gestión de incidentes de seguridad de la información
- 5.25 Evaluación y decisión en eventos de seguridad de la información
- 5.26 Respuesta a incidentes de seguridad de la información
- 5.27 Aprendizaje sobre los incidentes de seguridad de la información
- 5.28 Recopilación de evidencia
- 5.29 Seguridad de la información durante la ruptura
- 5.30 Preparación de las TIC para la continuidad del negocio

5. Controles Organizacionales

- 5.31 Requisitos contractuales, legales, estatutarios y regulatorios
- 5.32 Derechos de propiedad intelectual
- 5.33 Protección de registros
- 5.34 Privacidad y protección de la información de identificación personal
- 5.35 Revisión independiente de seguridad de la información
- 5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información
- 5.37 Procesos operativos documentados

6. Controles de Personas

- 6.1 Comprobaciones de verificación de antecedentes
- 6.2 Términos y condiciones para el empleo
- 6.3 Educación, entrenamiento y conciencia de seguridad de la información
- 6.4 Proceso disciplinario
- 6.5 Responsabilidades después de la terminación o cambio de empleo
- 6.6 Confidencialidad y no divulgación de acuerdos
- 6.7 Trabajo Remoto
- 6.8 Informes de eventos de seguridad de la información

7. Controles Físicos

- 7.1 Perímetros de seguridad física
- 7.2 Entradas físicas
- 7.3 Aseguramiento de oficinas, cuartos e instalaciones
- 7.4 Monitoreo de la seguridad física
- 7.5 Protección contra amenazas físicas y del entorno
- 7.6 Trabajo en áreas seguras
- 7.7 Escritorio y pantalla limpia
- 7.8 Protección y disposición de equipos
- 7.9 Seguridad de los activos fuera de las instalaciones
- 7.10 Medios de almacenamiento

7. Controles Físicos

- 7.11 Utilidades de apoyo
- 7.12 Seguridad del cableado
- 7.13 Equipos de mantenimiento
- 7.14 Eliminación segura o reutilización de equipo

8. Controles Tecnológicos

- 8.1 Dispositivos de usuario final
- 8.2 Derechos de acceso privilegiado
- 8.3 Restricción de acceso a la información
- 8.4 Acceso a código fuente
- 8.5 Autenticación segura
- 8.6 Gestión de la capacidad
- 8.7 Protección contra malware
- 8.8 Gestión de las vulnerabilidades técnicas
- 8.9 Gestión de la configuración
- 8.10 Eliminación de información

8. Controles Tecnológicos

- 8.11 Enmascaramiento de datos
- 8.12 Prevención de fuga de datos
- 8.13 Respaldo de información
- 8.14 Redundancia de las instalaciones de procesamiento de información
- 8.15 Inicio de sesión
- 8.16 Monitoreo de actividades
- 8.17 Sincronización de relojes
- 8.18 Uso de programas de utilidad privilegiados
- 8.19 Instalación de software en sistemas operativos
- 8.20 Seguridad de las redes

8. Controles Tecnológicos

- 8.21 Seguridad en los servicios de red
- 8.22 Segmentación de red
- 8.23 Filtrado web
- 8.24 Uso de criptografía
- 8.25 Seguridad en el ciclo de desarrollo
- 8.26 Requerimientos de seguridad en aplicaciones
- 8.27 Arquitectura segura y principios de seguridad para sistemas de información
- 8.28 Codificación segura
- 8.29 Pruebas de seguridad en desarrollo y aceptación de software
- 8.30 Desarrollo externo

8. Controles Tecnológicos

- 8.31 Separación de ambientes de desarrollo, pruebas y producción
- 8.32 Gestión de cambios
- 8.33 Información para pruebas
- 8.34 Protección de los sistemas de información durante las pruebas de auditoría

Taller 25 minutos

Revisar los Términos y Definiciones de Seguridad de la Información

Fase 3. Gestión de Riesgos de Seguridad de la Información Basado en ISO 27005

Esta norma suministra soporte a los conceptos que se especifican en la ISO-IEC 27001, la cual facilita la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

Esta norma se puede aplicar a todo tipo de Organizaciones que determine gestionar los riesgos de la seguridad de la información.

Gestión De Riesgos SGSI

Oportunidades: El propósito es gestionar/explotar las oportunidades de negocio y se enfoca en la inversión. De naturaleza ofensiva.

Impacto: Éxito de una vulnerabilidad por una amenaza en un activo al cual se le debe asignar un valor monetario estimado por rangos (por ej.: Entre U$ 1 y U$ 10 millones) se evalúa la probabilidad de ocurrencia del evento, por ej.: El virus es diario, semanal, etc. Clasificarlos en alto, medio o bajo. De naturaleza ofensiva.

Gestión De Riesgos SGSI

Riesgo del Negocio + Riesgos en los Sistemas de Información + Riesgos en los Procesos

Alta Gerencia — Aplicativos e Información — Usuario Final

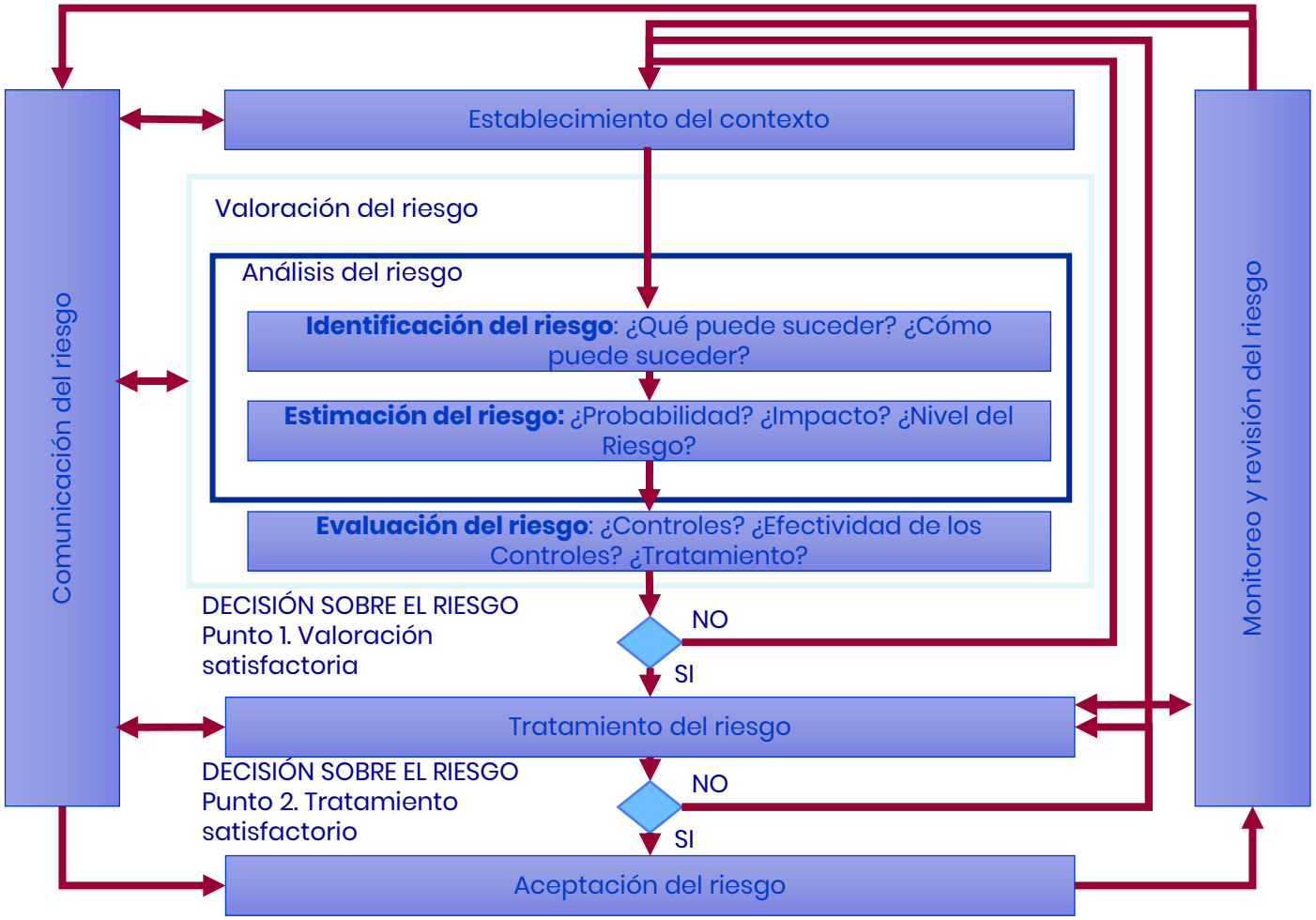
Controles a nivel transversal del negocio

¿Por Qué Realizar Una Gestión Al Riesgo?

Buscando eficiencia y eficacia de los procesos, un Sistema 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
- Su 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

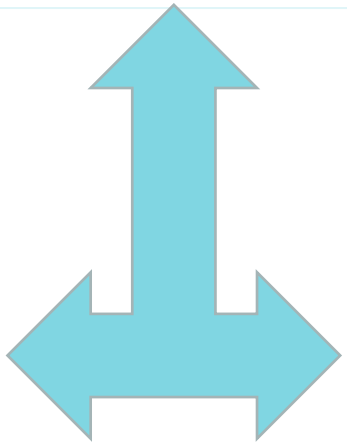
Proceso de Gestión del Riesgo Basado en ISO-IEC 27005



Establecimiento del Contexto

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 cultual
- 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 sicosociales

Identificación de los Activos

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)

Clasificación de los 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

Amenaza

Amenaza

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

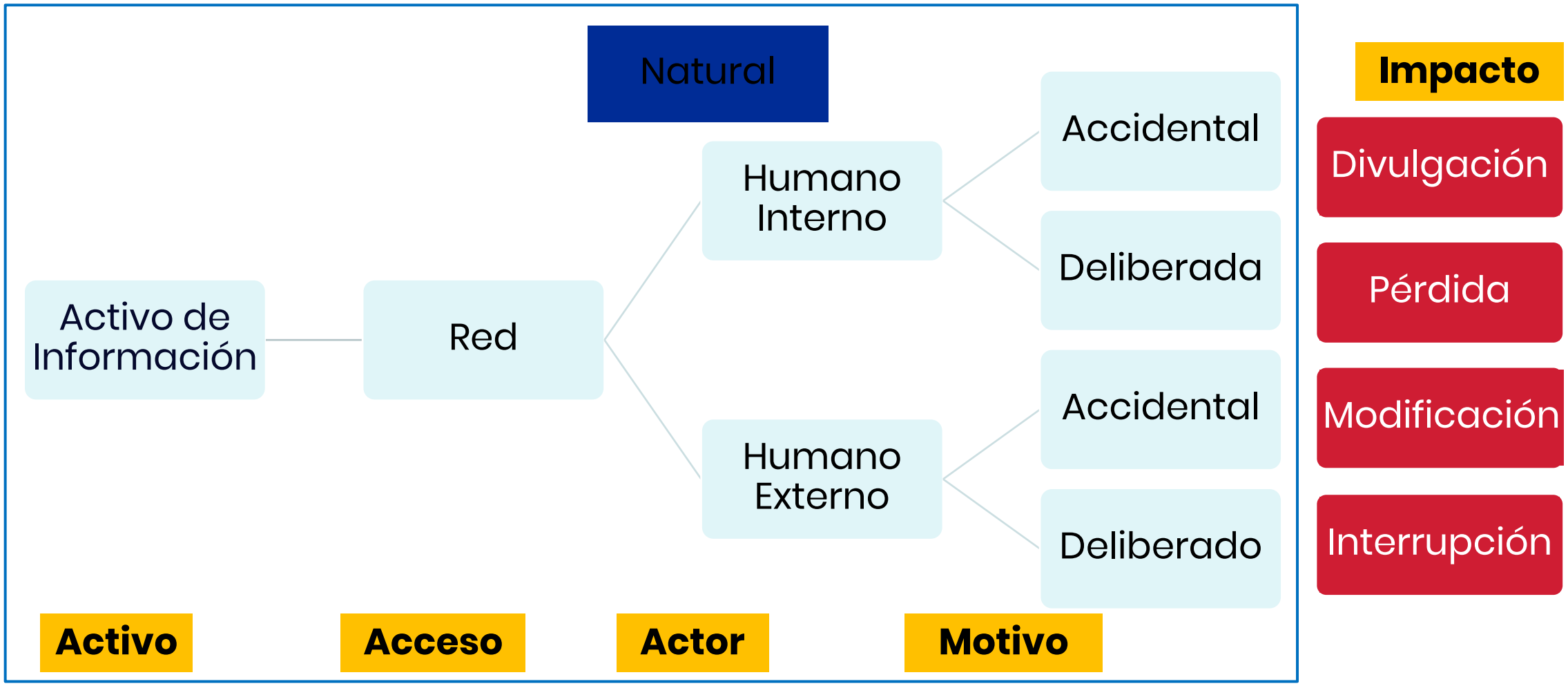
- Confidencialidad
- Disponibilidad
- Integridad

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.

Perfil de una Amenaza



Amenazas a la Información

Ejemplos:

- 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

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 → Gas.

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

Grado de sensibilidad de un Activo.

Vulnerabilidad

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 de S.O., DBMS 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.

Vulnerabilidad

Ejemplos

Actividad No.2 Riesgos de la Información		
ACTIVO DE INFORMACIÓN	**AMENAZA**	**VULNERABILIDAD**
Centro de cómputo	Inundación	Ubicación del Data Center en áreas cercanas a ríos, lagunas
Equipos de Comunicaciones	Pérdida de los servicios de T.I .	Ausencia de política de Continuidad del Negocio.
Recurso Humano	Pérdida de personal clave	Ausencia de planes de sucesión
Aplicativos "core del negocio"	Fallos de los procesos que afecten la Confidencialidad / Disponibilidad / Integridad.	Defectos de construcción de software

EJERCICIO : Desarrolle ejemplos prácticos de su labor asociando a los Activos de información sus respectivas Amenazas con sus Vulnerabilidades.

Se solicita desarrollar este ejercicio con los activos del Taller práctico No.1 Clasificación y valoración de Activos de Información.

Gestión de Riesgos SGSI: Taller

La empresa METALMECANICA S.A empezó sus actividades en 2010 con 150 empleados y con un mapa de procesos que hasta marzo de 2021 no estaba completamente definido.

Cuenta actualmente con unos aplicativos que no cubren completamente las actividades, aunque en reunión con la Gerencia, se manifiesta que hasta el momento todo ha funcionado muy bien aunque tienen procesos manuales. Desde sus inicios cuentan con la misma planta computacional y atendida por dos personas que tienen formación media profesional y atienden técnicamente las operaciones del negocio, con resultados satisfactorios.

En una auditoría realizada en el mes de abril, se concluye que las cifras financieras de la empresa son razonables. La Gerencia autoriza invertir en un proyecto de imagen Corporativa con el fin de posicionar la empresa en los medios y ante la competencia, este proyecto lo hace mediante crédito bancario. De acuerdo al anterior estado de METALMECANICA S.A se solicita desarrollar un ejercicio con Hallazgos, Amenazas, Vulnerabilidades.

Gestión de Riesgos SGSI: Taller

Solución

Hallazgo:

1. La empresa no cuenta con un mapa de procesos completamente definido, donde referencie sus actividades.
2.
3.

Amenazas:

1. Pérdida de los servicios de T.I.
2. Imposibilidad de atención a demandas de nuevos servicios
3.
4.

Vulnerabilidades:

1. Ausencia de políticas de caracterización de procesos
2. Ausencia de planes de desarrollo estratégico y tecnológico
3.
4.

Gestión de Riesgos SGSI: Taller

Su Organización está en riesgo cuando:

- Defectos o daños de cualquier activo de Información.
- Interrupciones no programadas.
- Modificación, interceptación o alteración de datos sin las debidas autorizaciones.

Además:

- Pérdida de operación o continuidad.
- Fallos o defectos sin previsión de la infraestructura de T.I.
- Imposibilidad de cumplir la promesa de servicio a los usarios Internos y externos.

Consultar otros factores de riesgo de T.I.

¿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).

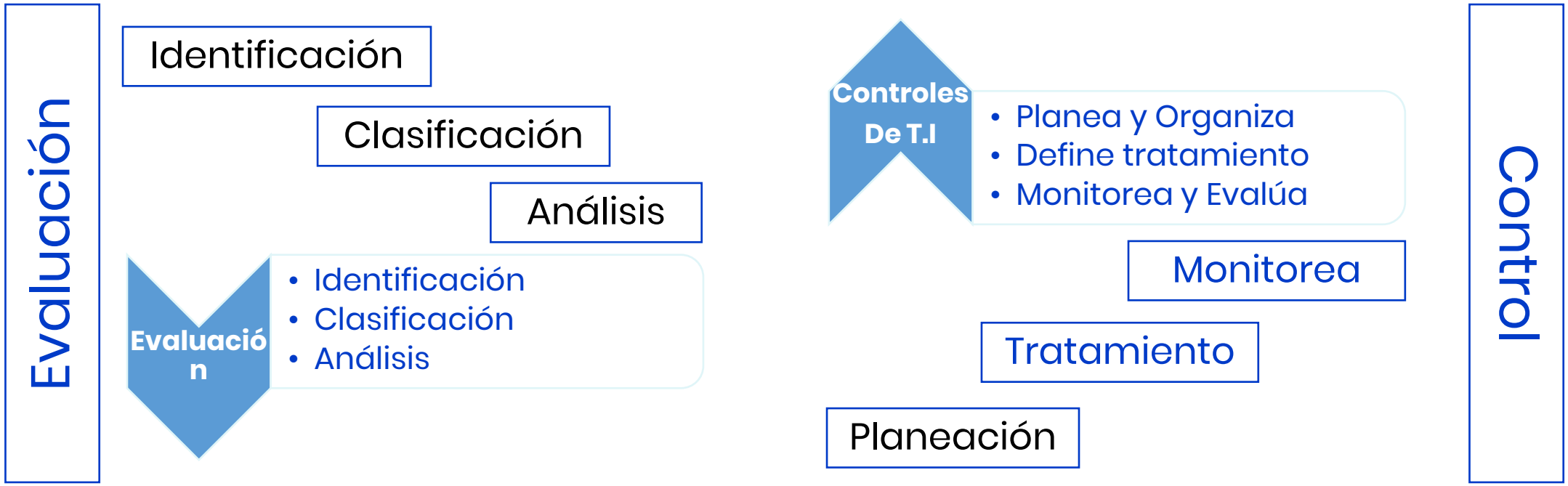
Puede ser positivo o negativo.

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

Controles:

- **M**itigar
- **E**vitar
- **T**ransferir
- **A**sumir

Ciclo de la Gestión de Riesgos



Gestión De Riesgos SGSI

Los siguientes 9 pasos llevará al participante a comprender el modelo de gestión de riesgos. Inicia en el CONTEXTO y finaliza en el diseño de LOS CONTROLES.

1. Establecimiento del contexto externo e interno
2. Clasificación de los activos de información

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

Gestión De Riesgos SGSI

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

3. Clasificación de amenazas y vulnerabilidades a los activos de información

Gestión De Riesgos SGSI

Activos de información

Amenazas 2021

Click →

Click ↓

4. Escenario de riesgos

Matriz que incluye los **Activos de Información** de la Organización.

Enfrentado con las **amenazas** para cada uno de los activos.

Amenazas 2021	Información Física I	Información Física 2	Herramientas para la Operación	Software Gestión	Red	Servidor Local	Equipo de computo	Almacenamiento	Conocimiento del negocio	CONFIDENCIALIDAD	DISPONIBILIDAD	INTEGRIDAD
Evento Natural	x	x			x		x					
Perdida de Servicios Esenciales					x	x	x					
Fallas Técnicas			x	x	x	x	x	x				
Daño Físico	x	x			x	x	x	x				
Ataques Informáticos					x	x	x	x	x			
Acciones No Autorizadas	x	x			x	x	x		x			
Compromiso de las Funciones									x			
Compromiso de la información	x	x	x	x			x		x			
Personal no satisfecho	x	x	x	x	x	x	x	x	x			
Tipología de activos de información	Documental		Software		Infraestructura		Equipos	Almacenamiento	Intangibles y RRHH	Seguridad de la información		

Gestión De Riesgos SGSI

5. Criterios de Riesgo

Tabla de Probabilidad / Frencuencia		
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 da 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

Gestión De Riesgos SGSI

6. Calificación escenarios de riesgos

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

Gestión De Riesgos SGSI

7. Mapa de riesgos

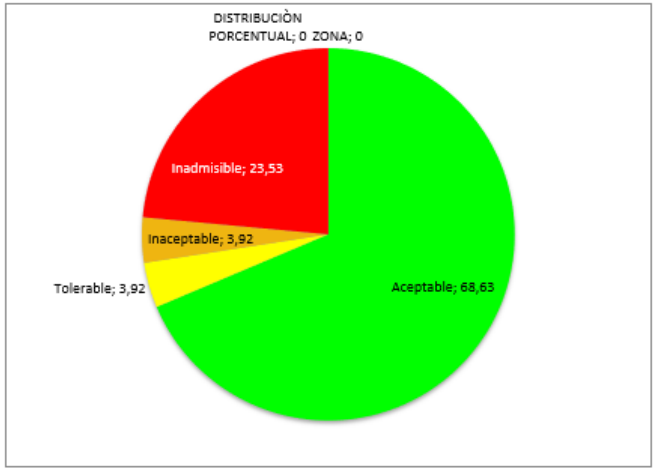
Matriz resultante del CRUCE Probabilidad X Impacto

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

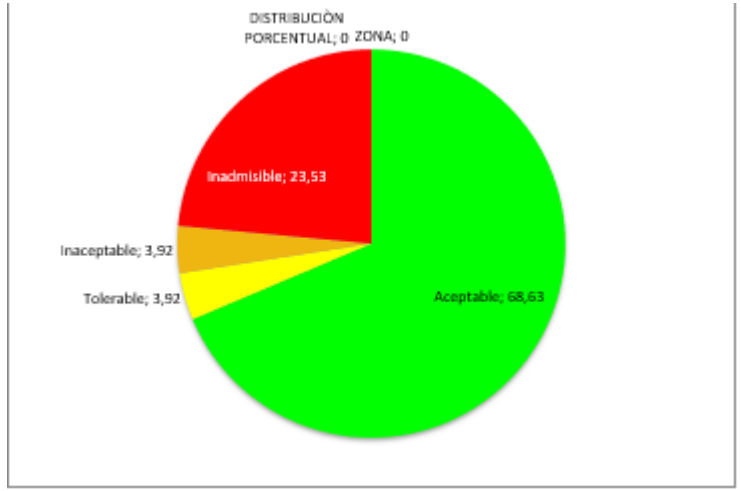


Gestión De Riesgos SGSI

8. 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 INFORMACIÓ - CONOCIMIENTO NEGOCIO ||
Posible	3		PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL || PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO ||		COMPROMISO DE LAS FUNCIONES - NOCIMIENTO NEGOCIO ||	ACCIONES NO AUTORIZADAS -- CONOCIMIENTO NEGOCIO || COMPROMISO DE LA INFORMACIÓ DOMINA DIGITAL F_E || COMPROMISO DE LA INFORMACIÓN -- SOFTWAR 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 -- ALMACEN MIENTO || 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

Gestión De Riesgos SGSI

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

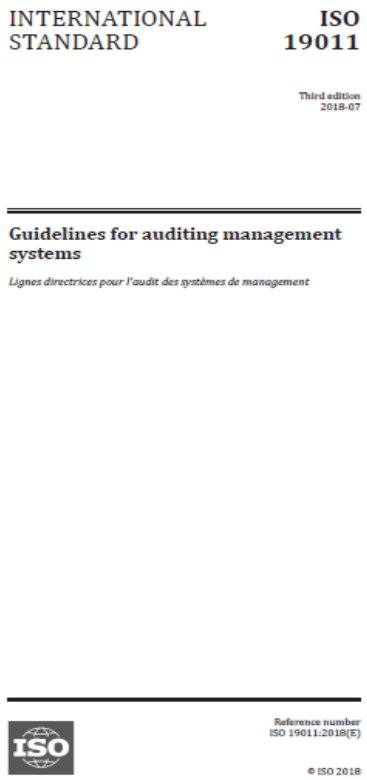
Gestión De Riesgos SGSI

9. Implementación de controles

Caracterización y atributos de los Controles

- Código Riesgo
- Categoría
- Nombre del riesgo
- Control
- Objetivo
- Guía de implementación
- Métricas
- Plan de monitoreo
- Responsable
- Resultado esperado
- Cronograma
- Presupuesto

Fase 4. Auditorías Internas con Énfasis en Competencias de Auditor Líder


INTERNATIONAL STANDARD

ISO 19011

Third edition
2018-07

Guidelines for auditing management systems

Lignes directrices pour l'audit des systèmes de management

Reference number
ISO 19011:2018(E)

© ISO 2018

Basado en la Norma ISO 19011

Esta norma proporciona una guía para todos los tamaños y tipos de organizaciones y auditorías de diferentes alcances y escalas, incluidas aquellas realizadas por grandes equipos de auditoría, generalmente de organizaciones más grandes, y aquellas realizadas por auditores individuales, ya sea en organizaciones grandes o pequeñas. Esta orientación debería adaptarse según corresponda al alcance, la complejidad y la escala del programa de auditoría.

Estructura de la 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

Alcance ISO 19011:2018

Este documento proporciona orientación sobre auditoría a sistemas de gestión, incluidos 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.

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.

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.

Tipos de Auditoría

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.

Tipos de Auditoría

A. **Auditorías internas:** a veces llamadas auditorías de primera parte son realizadas por o en nombre de la organización misma
B. **Auditorías externas:** incluyen aquellas generalmente llamadas auditorías de segunda y tercera parte

1. **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
2. **Auditorías de tercera parte:** son llevadas a cabo por organizaciones de auditoría independientes, como aquellas que proporcionan certificación / registro de conformidad o agencias gubernamentales

Criterios de Auditoría

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..

Evidencia de la Auditoría

- 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.

Resultados de la Auditoría

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 de entre los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina cumplimiento o incumplimiento.

Resultados de la Auditoría

- Hallazgo de cumplimiento
- Requisitos (norma, legal, reglamentario, contractual)
- El elemento se ajusta a la exigencia
- La implantación corresponde a la intención
- La implantación es eficaz

Mejores prácticas:

- Verificar los hechos verbales
- Definir la naturaleza de la no conformidad con el auditado, detallando la evidencia de auditoría
- Tomar notas y consultarlas posteriormente para realizar el reporte
- Hacer un bosquejo del reporte de hallazgos durante la toma de información
- Al finalizar cada jornada terminar en la revisión privada

Conclusiones de la Auditoría

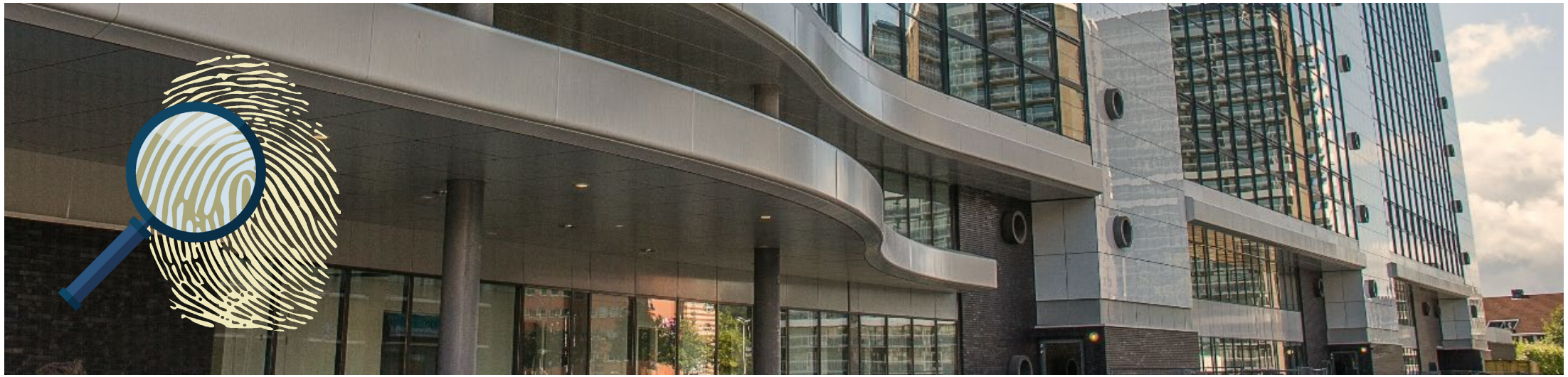
Resultado de una auditoría después de considerar los objetivos de auditoría y todos los resultados (hallazgos) de auditoría.

Cliente de la Auditoría

Organización o persona que solicita una auditoría.

•**Nota 1:** en el caso de la auditoría interna, el cliente de auditoría también puede ser el auditado o la persona(s) que administra el programa de auditoría. Las solicitudes de auditoría externa pueden provenir de fuentes tales como reguladores, partes contratantes o clientes potenciales o existentes.

Auditado



Organización en su totalidad o partes de ella siendo auditada.

Auditor

Persona que realiza una auditoría.

Equipo Auditor

Una o más personas que realizan una auditoría, apoyadas si es necesario por expertos técnicos.

- **Nota 1:** Un auditor del equipo de auditoría es designado como el líder del equipo de auditoría.
- **Nota 2:** El equipo de auditoría puede incluir auditores en capacitación.

Experto Técnico

Persona que proporciona conocimientos o experiencia específicos al equipo de auditoría.

- **Nota 1:** el conocimiento específico o experiencia se relaciona con la organización, la actividad, el proceso, el producto, el servicio, la disciplina que se auditará, el idioma o la cultura.

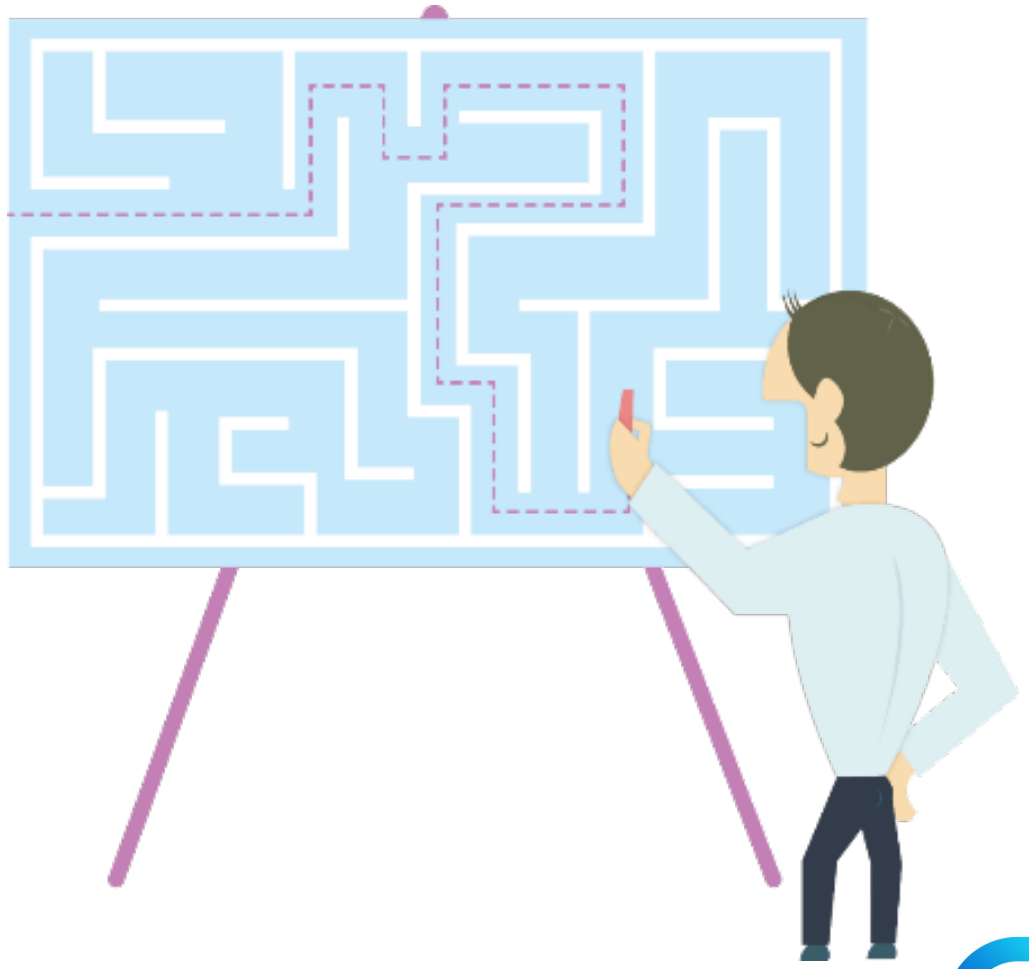
- **Nota 2:** Un experto técnico del equipo de auditoría no actúa como auditor.

Observador

Individuo que acompaña al equipo de auditoría pero que no actúa como auditor.

Guía

Persona designada por el auditado para asistir al equipo auditor.



Programa de Auditoría

Conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Alcance de la Auditoría

Alcance de auditoría se refiere al alcance y límites de una auditoría.

El alcance de la auditoría generalmente incluye una descripción de las ubicaciones físicas y virtuales, funciones, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto.

Una ubicación virtual es cuando una organización realiza un trabajo o proporciona un servicio usando un entorno en línea que permite a las personas, independientemente de las ubicaciones físicas, ejecutar procesos.

Plan de Auditoría

Descripción de las actividades y los arreglos para una auditoría.

Conformidad

Cumplimiento de un requisito.

No Conformidad

Incumplimiento de un requisito.

Pruebas de Auditoría

Registros, declaraciones de hechos u otra información, que sean relevantes para los criterios de auditoría y verificables.

Métodos de Auditoría

ALCANCE DE LA PARTICIPACIÓN ENTRE EL AUDITOR Y EL AUDITADO	Ubicación del Auditor	
	En el sitio	**Remota**
Interacción Humana	- Realización de entrevistas. - Completar listas de verificación y cuestionarios con participación del auditado. - Realización de una revisión de documentos con participación del auditado. - Muestreo.	**A través de comunicación interactiva significa:** - Realización de entrevistas. - Observar el trabajo realizado con la guía remota. - Completando listas de verificación y cuestionarios. - Realización de revisión de documentos con participación de los propietarios.
Sin Interacción Humana	- Realización de revisión de documentos (por ejemplo: registros, análisis de datos). - Observando el trabajo realizado. - Llevando a cabo una visita in-situ. - Completando listas de verificación. - Muestreo (por ejemplo: productos).	- Realización de revisión de documentos (por ejemplo: registros, análisis de datos). - Observar el trabajo realizado a través de medios de vigilancia, teniendo en cuenta los requisitos sociales, estatutarios y normativos. - Análisis de datos.

Las actividades de auditoría en el sitio se realizan en la ubicación del auditado. Las actividades de auditoría remota se realizan en cualquier lugar que no sea la ubicación del auditado, independientemente de la distancia. Las actividades de auditoría interactiva, implican la interacción entre el personal del auditado y el equipo de auditoría. Las actividades de auditoría no interactiva no implican interacción humana con las personas que representan al auditado, pero si implican la interacción con el equipo, las instalaciones y la documentación.

Cláusula 4: Principios de Auditoría

1. **Integridad**: la base del profesionalismo
2. **Presentación justa**: la obligación de informar veraz y exactamente
3. **Debido cuidado profesional**: la aplicación de la diligencia y el juicio en la auditoría
4. **Confidencialidad**: seguridad de la información
5. **Independencia:** la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría
6. **Enfoque basado en la evidencia**: el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático
7. **Enfoque basado en el riesgo**: un enfoque de auditoría que considera riesgos y oportunidades

Cláusula 4: Principios de Auditoría

Integridad: la base del profesionalismo

Los auditores y la (s) persona (s) que administran un programa de auditoría deberían:

a) Realizar su trabajo de forma ética, con honestidad y responsabilidad
b) Solo realizar actividades de auditoría si es competente para hacerlo
c) Realizar su trabajo de manera imparcial, es decir, seguir siendo justo e imparcial en todos sus tratos
d) Ser sensible a cualquier influencia que pueda ejercer sobre su juicio mientras lleva a cabo una auditoría

Cláusula 4: Principios de Auditoría

Presentación justa: la obligación de informar veraz y exactamente

Los hallazgos de la auditoría, las conclusiones de auditoría y los informes de auditoría deberían reflejar de manera veraz y precisa las actividades de auditoría. Se deberían informar los obstáculos significativos encontrados durante la auditoría y las opiniones divergentes no resueltas entre el equipo de auditoría y el auditado. La comunicación debería ser veraz, precisa, objetiva, oportuna, clara y completa.

Cláusula 4: Principios de Auditoría

Debido cuidado profesional: la aplicación de la diligencia y el juicio en la auditoría

Los auditores deberían tener el debido cuidado de acuerdo con la importancia de la tarea que realizan y la confianza depositada en ellos por el cliente de auditoría y otras partes interesadas. Un factor importante para llevar a cabo su trabajo con la debida atención profesional es tener la capacidad de emitir juicios razonados en todas las situaciones de auditoría.

Cláusula 4: Principios de Auditoría

Confidencialidad: seguridad de la información

Los auditores deberían ejercer discreción en el uso y la protección de la información adquirida en el desempeño de sus funciones. La información de auditoría no debería ser utilizada de manera inapropiada para beneficio personal por el auditor o el cliente de auditoría, o de una manera perjudicial para los intereses legítimos del auditado. Este concepto incluye el manejo adecuado de información sensible o confidencial.

Cláusula 4: Principios de Auditoría

Independencia: la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría

Los auditores deberían ser independientes de la actividad auditada siempre que sea posible y, en todos los casos, deberían actuar de forma tal que no estén sujetos a prejuicios ni a conflictos de intereses. Para las auditorías internas, los auditores deberían ser independientes de la función que se está auditando, si es posible. Los auditores deberían mantener la objetividad durante todo el proceso de auditoría para garantizar que los hallazgos y conclusiones de la auditoría se basen solo en la evidencia de auditoría.

Para las organizaciones pequeñas, puede que los auditores internos no sean totalmente independientes de la actividad que se audita, pero se deberían hacer todos los esfuerzos para eliminar el sesgo y alentar la objetividad.

Cláusula 4: Principios de Auditoría

Enfoque basado en la evidencia: el método racional para llegar a conclusiones de auditoría fiables y reproducibles en un proceso de auditoría sistemático

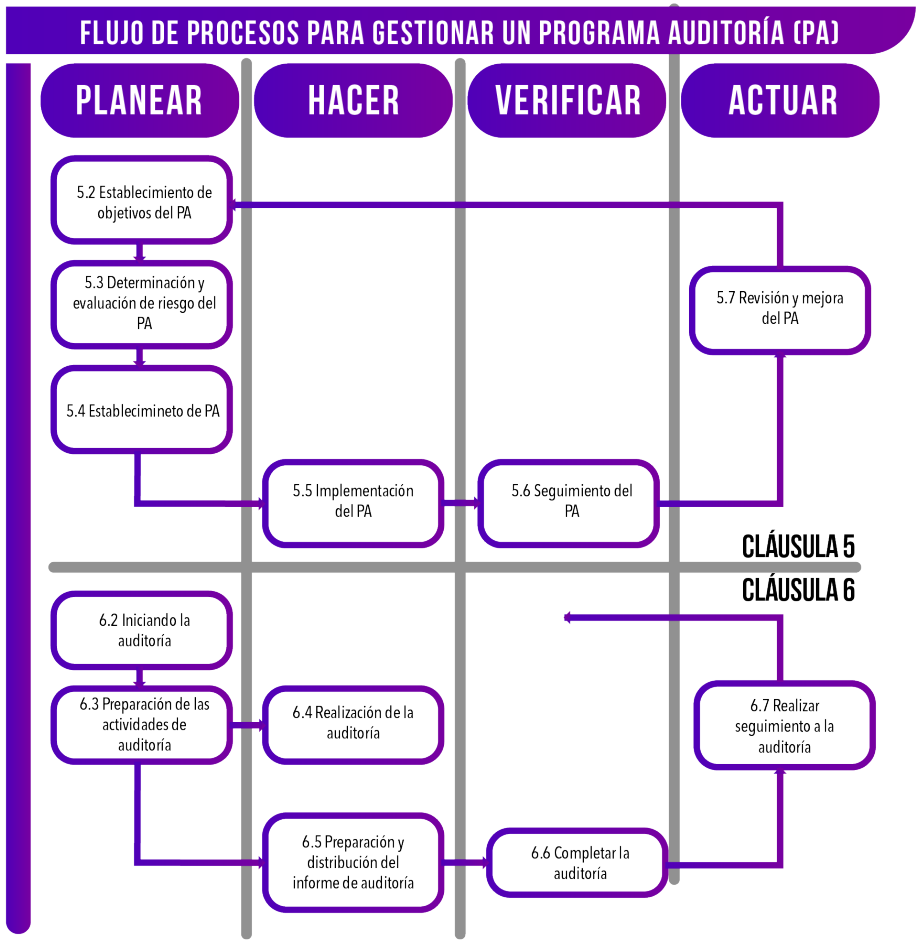
La evidencia de auditoría debería ser verificable. En general, debería basarse en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un tiempo finito y con recursos limitados. Se debería aplicar un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que se puede depositar en las conclusiones de la auditoría.

Cláusula 4: Principios de Auditoría

Enfoque basado en el riesgo: un enfoque de auditoría que considera riesgos y oportunidades

El enfoque basado en el riesgo debería influir sustancialmente en la planificación, conducción y presentación de informes de las auditorías para garantizar que las auditorías se centren en asuntos que son importantes para el cliente de auditoría y para lograr los objetivos del programa de auditoría.

Cláusula 5: Programa de Auditoría



NOTA 1: Esta figura ilustra la aplicación Planear – Hacer – Verificar – Actuar, en este documento.

NOTA 2: La numeración de cláusulas/subcláusulas se refiere a las cláusulas/subcláusulas relevantes de este documento.

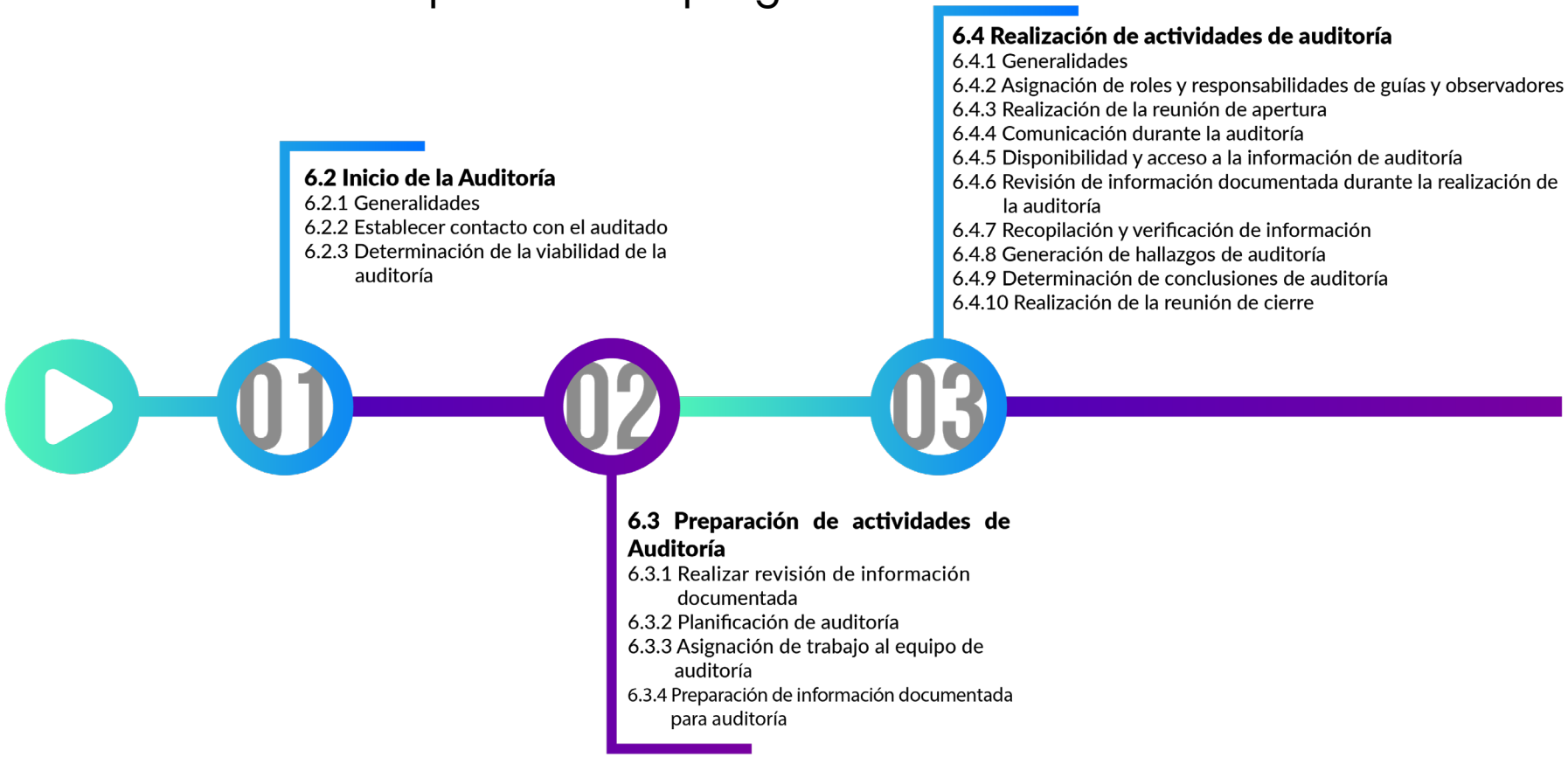
Figura 1: Flujo de proceso para la gestión de un programa de auditoría.

Cláusula 5: Programa de Auditoría

AUDITORÍAS	MES 1	MES 2	MES 3	MES 4	MES 5
Auditoría 1					
Auditoría 2					
Auditoría 3					

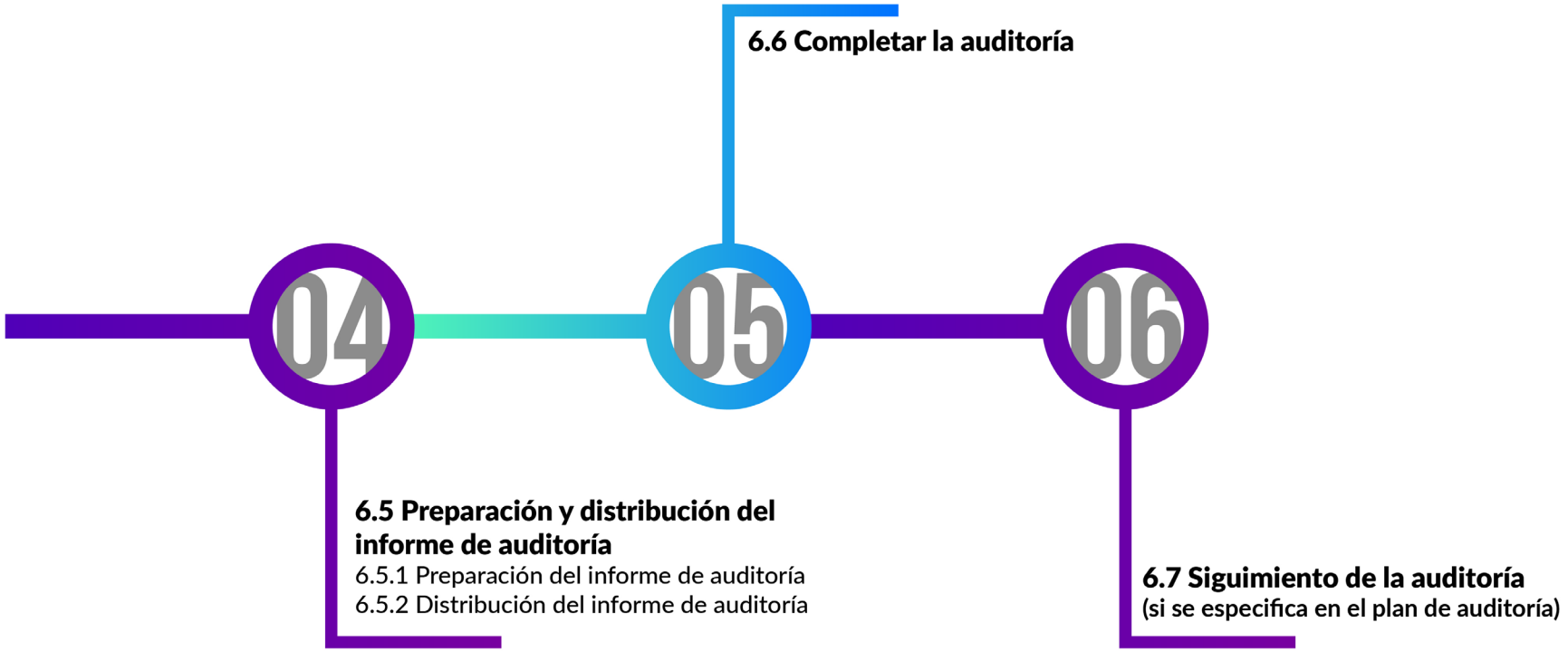
Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.



Cláusula 6: Actividades de la Auditoría

Esta cláusula proporciona orientación sobre la planificación y la forma de llevar a cabo las actividades de auditoría como parte de un programa de auditoría.



Cláusula 6: Actividades de la Auditoría

El líder del equipo auditor debería: Realizar reuniones informativas del equipo auditor, cuando sea apropiado, para distribuir las asignaciones de trabajo y decidir los posibles cambios.

Cláusula 7: Competencia y Evaluación de los Auditores

Esta cláusula trata las competencias de los auditores al realizar una auditoría. Los auditores deben:

- Poseer cualidades personales, tales como diplomacia, sinceridad, percepción, persistencia, etc. para que la auditoría se realice en forma profesional y correcta a la vez
- Poseer conocimientos genéricos y habilidades tales como:
  - Aplicar principios, procedimientos y técnicas de auditoría
  - Planificar y organizar el trabajo en forma eficaz
  - Conocer los códigos, leyes y normativas locales, regionales y nacionales

Cláusula 7: Competencia y Evaluación de los Auditores

Poseer un adecuado nivel de educación, experiencia laboral, capacitación como auditor y experiencia en auditorías.

Mantener y mejorar en forma continua sus habilidades y competencias.

Métodos para Evaluar a los Auditores

MÉTODO DE EVALUACIÓN	OBJETIVOS	EJEMPLOS
REVISIÓN DE REGISTROS	Verificar los antecedentes del auditor.	Análisis de registros de educación, capacitación, empleo, credenciales profesionales y experiencia en auditoría.
RETROALIMENTACIÓN	Obtener / proporcionar información sobre cómo se percibe el desempeño del auditor.	Encuestas, cuestionarios, referencias personales, testimonios, reclamos, evaluación de desempeño, revisión por pares.
ENTREVISTA	Evaluar el comportamiento profesional deseado y las habilidades de comunicación. Verificar la información y probar el conocimiento y adquirir información adicional.	Entrevistas personales.
OBSERVACIÓN	Evaluar el comportamiento profesional deseado y la capacidad de aplicar los conocimientos y las habilidades.	Role playing, auditorías atestiguadas, desempeño en el trabajo.
PRUEBAS	Evaluar el comportamiento deseado, el conocimiento, las habilidades y su aplicación.	Exámenes orales y escritos, pruebas psicométricas.
REVISIÓN POSTERIOR A LA AUDITORÍA	Proporcionar información sobre el desempeño del auditor durante las actividades de auditoría, indentificar fortalezas y oportunidades de mejora.	Revisión del informe de auditoría, entrevistas con el líder del equipo de auditoría, el equio de auditoría y si corresponde, retroalimentación del auditado.

Cláusula 7: Atributos Personales

a) **Ético,** es decir, justo, veraz, sincero, honesto y discreto
b) **De mente abierta**, es decir, dispuesto a considerar ideas o puntos de vista alternativos
c) **Diplomático**, es decir, discreto al tratar con individuos
d) **Observador**, es decir, observando activamente el entorno físico y las actividades
e) **Perceptivo**, es decir, consciente de y capaz de comprender situaciones
f) **Versátil**, es decir, capaz de adaptarse fácilmente a diferentes situaciones
g) **Tenaz**, es decir persistente y enfocado en alcanzar objetivos

Cláusula 7: Atributos Personales

h. **Decisivo**, es decir, capaz de llegar a conclusiones oportunas basadas en el razonamiento lógico y el análisis
i. **Autosuficiente**, es decir, capaz de actuar y funcionar independientemente mientras interactúa efectivamente con otros
j. **Capaz de actuar con fortaleza**, es decir, capaz de actuar de manera responsable y ética, aunque estas acciones no siempre sean populares y en ocasiones pueden dar lugar a desacuerdos o confrontaciones
k. **Abierto a la mejora**, es decir, dispuesto a aprender de las situaciones
l. **Culturalmente sensible**, es decir, atento y respetuoso con la cultura del auditado
m. **Colaborador**, es decir, interacción efectiva con otros, incluidos los miembros del equipo de auditoría y el personal del auditado

Cláusula 7: Conocimientos Genéricos y Habilidades

a) Los auditores deberían tener conocimiento y habilidades en las áreas que se detallan a continuación: Principios, procesos y métodos de auditoría: el conocimiento y las habilidades en esta área le permiten al auditor asegurar que las auditorías se realicen de manera consistente y sistemática.

Un auditor debería ser capaz de:

- Comprender los tipos de riesgos y oportunidades asociados con la auditoría y los principios del enfoque de auditoría basado en el riesgo
- Planificar y organizar el trabajo de manera efectiva
- Realizar la auditoría dentro del cronograma acordado
- Priorizar y enfocarse en asuntos importantes
- Comunicarse de manera efectiva, oralmente y por escrito (ya sea personalmente o mediante el uso de intérpretes)
- Recopilar información mediante entrevistas efectivas, escuchar, observar y revisar información documentada, incluidos registros y datos

Cláusula 7: Conocimientos Genéricos y Habilidades

Un auditor debería ser capaz de:

- Comprender la idoneidad y las consecuencias del uso de técnicas de muestreo para la auditoría
- Entender y considerar las opiniones de los expertos técnicos
- Auditar un proceso de principio a fin, incluidas las interrelaciones con otros procesos y diferentes funciones, según corresponda
- Verificar la relevancia y exactitud de la información recopilada
- Confirmar la suficiencia e idoneidad de la evidencia de auditoría para respaldar los hallazgos y conclusiones de la auditoría
- Evaluar aquellos factores que pueden afectar la confiabilidad de los hallazgos y conclusiones de la auditoría
- Documentar las actividades de auditoría y los hallazgos de auditoría, y preparar informes
- Mantener la confidencialidad y seguridad de la información

Cláusula 7: Conocimientos Genéricos y Habilidades

b) Normas del sistema de gestión y otras referencias: el conocimiento y las habilidades en esta área le permiten al auditor comprender el alcance de la auditoría y aplicar criterios de auditoría, y deberían cubrir lo siguiente:

- Normas del sistema de gestión u otros documentos normativos u orientativos/de apoyo utilizados para establecer criterios o métodos de auditoría
- La aplicación de los estándares del sistema de gestión por el auditado y otras organizaciones
- Relaciones e interacciones entre los procesos del sistema de gestión
- Comprender la importancia y la prioridad de múltiples estándares o referencias
- Aplicación de estándares o referencias a diferentes situaciones de auditoría

Cláusula 7: Conocimientos Genéricos y Habilidades

c) La organización y su contexto: el conocimiento y las habilidades en esta área le permiten al auditor comprender la estructura, el propósito y las prácticas de gestión del auditado y debería cubrir lo siguiente:

- Necesidades y expectativas de las partes interesadas relevantes que impactan en el sistema de gestión
- Tipo de organización, gobierno, tamaño, estructura, funciones y relaciones
- Conceptos generales de negocios y gestión, procesos y terminología relacionada, incluida la planificación, presupuestación y gestión de personas
- Aspectos culturales y sociales del auditado

Cláusula 7: Conocimientos Genéricos y Habilidades

d) Requisitos reglamentarios y legales aplicables y otros requisitos: el conocimiento y las habilidades en esta área le permiten al auditor conocer y trabajar dentro de los requisitos de la organización. Los conocimientos y habilidades específicos de la jurisdicción o de las actividades, procesos, productos y servicios del auditado deberían cubrir lo siguiente:

- Requisitos legales y reglamentarios, así como sus agencias de gobierno
- Terminología jurídica básica
- Contratación y responsabilidad

NOTA: La conciencia de los requisitos legales y reglamentarios no implica pericia legal y una auditoría del sistema de gestión no debería tratarse como una auditoría de cumplimiento legal.

Cláusula 7: Conocimientos Genéricos y Habilidades

La 19011 lo define como arreglos para un conjunto de una o más auditorías planificadas para un marco de tiempo específico y dirigidas hacia un propósito específico.

- Un programa de auditoría puede incluir una o más auditorías, dependiendo del tamaño, la naturaleza y la complejidad de la organización que va a ser auditada
- El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza del auditado, así como en la naturaleza, funcionalidad, complejidad, el tipo de riesgos y oportunidades, y el nivel de madurez de los sistemas de gestión a ser auditados
- Para comprender el contexto del auditado, el programa de auditoría debería tener en cuenta:
  - Objetivos organizacionales
  - Cuestiones externas e internas relevantes
  - Las necesidades y expectativas de las partes interesadas pertinentes
  - Requisitos de confidencialidad y seguridad de la información

Establecimiento de Objetivos del Programa de Auditoría

El cliente de auditoría debería asegurarse de que los objetivos del programa de auditoría se establezcan para dirigir la planificación y la realización de auditorías, y debería garantizar que el programa de auditoría se implemente de manera efectiva.

Los objetivos del programa de auditoría deberían ser coherentes con la orientación estratégica y los objetivos y la política del sistema de gestión de soporte del cliente de auditoría.

Estos objetivos pueden basarse en la consideración de lo siguiente:

a) Las necesidades y expectativas de las partes interesadas pertinentes, tanto externas como internas
b) Características y requisitos de procesos, productos, servicios y proyectos, y cualquier cambio en ellos
c) Requisitos del sistema de gestión
d) Necesidad de evaluación de proveedores externos
e) El nivel de rendimiento y el nivel de madurez del sistema o sistemas de gestión del auditado, como se refleja en los indicadores de rendimiento relevantes (por ejemplo, KPI's), la ocurrencia de no conformidades, incidentes o quejas de las partes interesadas
f) Identificó riesgos y oportunidades para el auditado
g) Resultados de auditorías anteriores

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Existen riesgos y oportunidades relacionados con el contexto del auditado que pueden asociarse con un programa de auditoría y pueden afectar el logro de sus objetivos.

La persona responsable del programa de auditoría **debería considerar los riesgos** durante el desarrollo del programa:

a) **Planificación**, por ejemplo; no establecer los objetivos de auditoría relevantes y determinar el alcance, el número, la duración, las ubicaciones y el cronograma de las auditorías
b) **Recursos,** por ejemplo; permitir tiempo, equipo y/o capacitación insuficientes para desarrollar el programa de auditoría o realizar una auditoría
c) **Selección del equipo de auditoría,** por ejemplo; competencia global insuficiente para realizar auditorías de manera efectiva
d) **Comunicación**, por ejemplo; procesos/canales de comunicación externos/internos ineficaces

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

e) **Implementación**, por ejemplo; coordinación ineficaz de las auditorías dentro del programa de auditoría, o no considerar la seguridad y confidencialidad de la información

f) **Control de la información documentada**, por ejemplo; la determinación ineficaz de la información documentada necesaria requerida por los auditores y las partes interesadas pertinentes; la falta de protección adecuada de los registros de auditoría para demostrar la eficacia del programa de auditoría

g) **Supervisar, revisar y mejorar el programa de auditoría**, por ejemplo; seguimiento ineficaz de los resultados del programa de auditoría

h) **Disponibilidad y cooperación del auditado** y disponibilidad de evidencia para ser muestreada

Determinación y Evaluación de Riesgos y Oportunidades del Programa de Auditoría

Las oportunidades para mejorar el programa de auditoría pueden incluir:

a) Permitir múltiples auditorías en una sola visita
b) Minimizar el tiempo y las distancias que viajan al sitio
c) Hacer coincidir el nivel de competencia del equipo de auditoría con el nivel de competencia necesario para alcanzar los objetivos de la auditoría
d) Alinear las fechas de auditoría con la disponibilidad del personal clave del auditado

Establecimiento del Programa de Auditoría

Roles y responsabilidades de las personas que gestionan el programa de auditoría

a) Establecer la extensión del programa de auditoría de acuerdo con los objetivos relevantes y cualquier restricción conocida
b) Determinar los problemas externos e internos, y los riesgos y oportunidades que pueden afectar el programa de auditoría, e implementar acciones para abordarlos, integrando estas acciones en todas las actividades de auditoría relevantes, según corresponda
c) Garantizar la selección de los equipos de auditoría y la competencia general para las actividades de auditoría mediante la asignación de funciones, responsabilidades y autoridades, y el apoyo al liderazgo, según corresponda

Establecimiento del Programa de Auditoría

Roles y responsabilidades de las personas que gestionan el programa de auditoría

d) Establecer todos los procesos relevantes, incluidos los procesos para:

- La coordinación y programación de todas las auditorías dentro del programa de auditoría
- El establecimiento de objetivos de auditoría, alcance (s) y criterios de las auditorías, determinación de los métodos de auditoría y selección del equipo de auditoría
- Evaluación de auditores
- El establecimiento de procesos de comunicación externa e interna, según corresponda
- La resolución de disputas y el manejo de quejas
- Seguimiento de auditoría si corresponde
- Informar al cliente de auditoría y a las partes interesadas pertinentes, según corresponda

Establecimiento del Programa de Auditoría

Roles y responsabilidades de las personas que gestionan el programa de auditoría

e) Determinar y garantizar la provisión de todos los recursos necesarios
f) Garantizar que se prepare y mantenga la información documentada apropiada, incluidos los registros del programa de auditoría
g) Monitorear, revisar y mejorar el programa de auditoría
h) Comunicar el programa de auditoría al cliente de auditoría y, según corresponda, a las partes interesadas pertinentes

Las personas que gestionan el programa de auditoría deberían solicitar su aprobación al cliente de auditoría.

Competencia de (los) Individuo(s) que Gestiona(n) el Programa de Auditoría

La(s) persona(s) que gestiona(n) el programa de auditoría deberían tener la competencia necesaria para gestionar el programa, sus riesgos y oportunidades asociados y los problemas externos e internos de manera efectiva y eficiente, incluido el conocimiento de:

a) Principios de auditoría, métodos y procesos
b) Normas del sistema de gestión, otras normas pertinentes y documentos de referencia / orientación
c) Información sobre el auditado y su contexto (por ejemplo, asuntos externos/internos, partes interesadas relevantes y sus necesidades y expectativas, actividades comerciales, productos, servicios y procesos del auditado
d) Requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades comerciales del auditado

Establecer el Alcance del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían determinar el alcance del programa de auditoría. Esto puede variar según la información proporcionada por el auditado con respecto a su contexto.

Otros factores que impactan en el alcance del programa de auditoría:

a) El objetivo, el alcance y la duración de cada auditoría y la cantidad de auditorías que se llevarán a cabo, el método de notificación y, si corresponde, el seguimiento de la auditoría
b) Las normas del sistema de gestión u otros criterios aplicables
c) El número, la importancia, la complejidad, la similitud y la ubicación de las actividades a auditar

Establecer el Alcance del Programa de Auditoría

d) Aquellos factores que influyen en la efectividad del sistema de gestión
e) Los criterios de auditoría aplicables, tales como los arreglos planificados para las normas del sistema de gestión pertinentes, los requisitos legales y reglamentarios y otros requisitos con los que la organización está comprometida
f) Resultados de auditorías internas o externas previas y revisiones de la dirección, si corresponde
g) Resultados de una revisión previa del programa de auditoría
h) Problemas lingüísticos, culturales y sociales
i) Las preocupaciones de las partes interesadas, tales como las quejas de los clientes, el incumplimiento de los requisitos legales y reglamentarios y otros requisitos con los que la organización se compromete, o los problemas de la cadena de suministro

Establecer el Alcance del Programa de Auditoría

j) Cambios significativos en el contexto del auditado o sus operaciones y riesgos y oportunidades relacionados

k) Disponibilidad de tecnologías de información y comunicación para respaldar las actividades de auditoría, en particular el uso de métodos de auditoría remota

l) La ocurrencia de eventos internos y externos, tales como no conformidades de productos o servicios, fugas de seguridad de la información, incidentes de salud y seguridad, actos delictivos o incidentes ambientales

m) Riesgos y oportunidades comerciales, incluidas las acciones para abordarlos

Determinar los Recursos del Programa de Auditoría

Al determinar los recursos para el programa de auditoría, las personas que gestionan el programa de auditoría deberían considerar:

a) Los recursos financieros y de tiempo necesarios para desarrollar, implementar, administrar y mejorar las actividades de auditoría
b) Métodos de auditoría
c) La disponibilidad individual y general de auditores y expertos técnicos que posean las competencias apropiadas para los objetivos particulares del programa de auditoría
d) La extensión del programa de auditoría y los riesgos y oportunidades del programa de auditoría.
e) Tiempo de viaje y costo, alojamiento y otras necesidades de auditoría

Determinar los Recursos del Programa de Auditoría

f) El impacto de las diferentes zonas horarias
g) La disponibilidad de tecnologías de información y comunicación (por ejemplo, los recursos técnicos necesarios para establecer una auditoría remota utilizando tecnologías que admiten la colaboración remota)
h) La disponibilidad de cualquier herramienta, tecnología y equipo requerido
i) La disponibilidad de la información documentada necesaria, según se determine durante el establecimiento del programa de auditoría
j) Los requisitos relacionados con la instalación, incluidos los espacios de seguridad y el equipo (por ejemplo, equipo de protección personal entre otras)

Implementación del Programa de Auditoría

a) Comunicar las partes pertinentes del programa de auditoría, incluidos los riesgos y oportunidades, a las partes interesadas pertinentes e informarles periódicamente de su progreso, utilizando los canales de comunicación externos e internos establecidos
b) Definir objetivos, alcance y criterios para cada auditoría individual
c) Seleccionar métodos de auditoría
d) Coordinar y programar auditorías y otras actividades relevantes para el programa de auditoría
e) Garantizar que los equipos de auditoría tengan la competencia necesaria
f) Proporcionar los recursos individuales y globales necesarios a los equipos de auditoría
g) Garantizar la realización de auditorías de acuerdo con el programa de auditoría, gestionando todos los riesgos, oportunidades y problemas operativos (es decir, eventos inesperados), tal como surgen durante el despliegue del programa
h) Garantizar que la información documentada relevante con respecto a las actividades de auditoría se gestiona y mantiene de forma adecuada
i) Definir e implementar los controles operativos necesarios para la supervisión del programa de auditoría
j) Revisar el programa de auditoría para identificar oportunidades para su mejora

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

Cada auditoría individual debería basarse en objetivos de auditoría definidos, alcance y criterios. Estos deberían ser consistentes con los objetivos generales del programa de auditoría.

Los objetivos de la auditoría definen que se va a lograr con la auditoría individual y pueden incluir lo siguiente:

a) Determinación del grado de conformidad del sistema de gestión a ser auditado, o partes de él, con los criterios de auditoría
b) Evaluación de la capacidad del sistema de gestión para ayudar a la organización a cumplir los requisitos legales y reglamentarios pertinentes y otros requisitos con los que la organización está comprometida
c) Evaluación de la efectividad del sistema de gestión para alcanzar los resultados esperados

Definición de Objetivos, Alcance y Criterios para una Auditoría Individual

d) Identificación de oportunidades para la mejora potencial del sistema de gestión
e) Evaluación de la idoneidad y adecuación del sistema de gestión con respecto al contexto y la dirección estratégica del auditado
f) Evaluación de la capacidad del sistema de gestión para establecer y alcanzar objetivos y abordar de manera efectiva los riesgos y oportunidades, en un contexto cambiante, incluida la implementación de las acciones relacionadas

El alcance de la auditoría debería ser coherente con el programa de auditoría y los objetivos de auditoría.

Selección y Determinación de Métodos de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) seleccionar y determinar los métodos para llevar a cabo eficazmente y de manera eficiente una auditoría, dependiendo de los objetivos de auditoría definidos, el alcance y criterios.

Las auditorías pueden realizarse en el sitio, de forma remota o como una combinación. El uso de estos métodos debería estar adecuadamente equilibrado, en función de, entre otros, la consideración de los riesgos y oportunidades asociados.

Si un auditado opera dos o más sistemas de gestión de diferentes disciplinas, se pueden incluir auditorías combinadas en el programa de auditoría.

Selección de los Miembros del Equipo de Auditoría

El(los) individuo(s) que gestiona(n) el programa de auditoría debería(n) nombrar a los miembros del equipo de auditoría, incluyendo el líder del equipo y cualquier expertos técnicos necesarios para la auditoría específica.

Se debería seleccionar un equipo de auditoría, teniendo en cuenta la competencia necesaria para alcanzar los objetivos de la auditoría individual dentro del alcance definido. Si solo hay un auditor, el auditor debería realizar todas las tareas aplicables de un líder del equipo de auditoría.

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

Las personas que gestionan el programa de auditoría deberían asignar la responsabilidad de llevar a cabo la auditoría individual a un líder del equipo de auditoría.

La asignación debería hacerse con suficiente tiempo antes de la fecha programada de la auditoría, a fin de garantizar la planificación efectiva de la auditoría.

Para que la auditoría se lleve a cabo eficazmente, se deberá proporcionar al auditor líder información sobre:

a) Objetivos de auditoría
b) Criterios de auditoría y cualquier información documentada relevante
c) Alcance de la auditoría, incluida la identificación de la organización y sus funciones y procesos a auditar

Asignación de Responsabilidades al Líder del Equipo Auditor para una Auditoría Individual

d) Procesos de auditoría y métodos asociados
e) Composición del equipo de auditoría
f) Los datos de contacto del auditado, las ubicaciones, el marco temporal y la duración de las actividades de auditoría que se llevarán a cabo
g) Los recursos necesarios para llevar a cabo la auditoría
h) Información necesaria para evaluar y abordar los riesgos y oportunidades identificados para el logro de los objetivos de la auditoría
i) Información que respalda al (los) líder (es) del equipo de auditoría en sus interacciones con el auditado para la efectividad del programa de auditoría

Gestión de los Resultados del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar que se realicen las siguientes actividades:

a) Evaluación del logro de los objetivos para cada auditoría dentro del programa de auditoría
b) Revisión y aprobación de informes de auditoría sobre el cumplimiento del alcance y los objetivos de la auditoría
c) Revisión de la efectividad de las acciones tomadas para abordar los hallazgos de auditoría
d) Distribución de informes de auditoría a las partes interesadas pertinentes
e) Determinación de la necesidad de cualquier auditoría de seguimiento

La persona que administra el programa de auditoría debería considerar, cuando corresponda:

- Comunicar los resultados de auditoría y las mejores prácticas a otras áreas de la organización
- Las implicaciones para otros procesos

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que administran el programa de auditoría deberían garantizar que los registros de auditoría se generen, administren y mantengan para demostrar la implementación del programa de auditoría.

Los registros pueden incluir lo siguiente:

a) Registros relacionados con el programa de auditoría, tales como:
   - Calendario de auditorías
   - Objetivos y alcance del programa de auditoría
   - Aquellos que abordan los riesgos y oportunidades del programa de auditoría, y los problemas externos e internos relevantes
   - Revisiones de la efectividad del programa de auditoría

Administrar y Mantener los Registros del Programa de Auditoría

b) Registros relacionados con cada auditoría, tales como:
   - Planes de auditoría e informes de auditoría
   - Evidencia de auditoría objetiva y hallazgos
   - Informes de no conformidad
   - Correcciones e informes de acciones correctivas
   - Informes de seguimiento de auditoría

c) Registros relacionados con el equipo de auditoría que cubren temas tales como:
   - Evaluación de competencia y desempeño de los miembros del equipo de auditoría
   - Criterios para la selección de equipos de auditoría y miembros del equipo y formación de equipos de auditoría
   - Mantenimiento y mejora de la competencia

Administrar y Mantener los Registros del Programa de Auditoría

Las personas que gestionan el programa de auditoría deberían garantizar la evaluación de:

a) Sí se están cumpliendo los cronogramas y si se están logrando los objetivos del programa de auditoría
b) El desempeño de los miembros del equipo de auditoría, incluido el líder del equipo de auditoría y los expertos técnicos
c) La capacidad de los equipos de auditoría para implementar el plan de auditoría
d) Retroalimentación de clientes de auditoría, auditados, auditores, expertos técnicos y otras partes relevantes
e) Suficiencia y adecuación de la información documentada en todo el proceso de auditoría

Revisión y Mejora del Programa de Auditoría

Las personas que gestionan el programa de auditoría y el cliente de auditoría deberían revisar el programa de auditoría para evaluar si se han alcanzado sus objetivos.

La revisión del programa de auditoría debería considerar lo siguiente:

a) Resultados y tendencias del seguimiento del programa de auditoría
b) Conformidad con los procesos del programa de auditoría e información documentada relevante
c) La evolución de las necesidades y expectativas de las partes interesadas pertinentes
d) Registros del programa de auditoría
e) Métodos de auditoría alternativos o nuevos
f) Métodos alternativos o nuevos para evaluar a los auditores
g) Efectividad de las acciones para abordar los riesgos y oportunidades, y problemas internos y externos asociados con el programa de auditoría
h) Cuestiones de confidencialidad y seguridad de la información relacionadas con el programa de auditoría

Establecer Contacto con el Auditado

Es responsabilidad del auditor líder.

Propósito

a) Confirmar los canales de comunicación con los representantes del auditado
b) Confirmar la autoridad para realizar la auditoría
c) Proporcionar información relevante sobre los objetivos, el alcance, los criterios, los métodos y la composición del equipo de auditoría, incluidos los expertos técnicos
d) Solicitar acceso a información relevante para fines de planificación, incluida información sobre los riesgos y oportunidades que la organización ha identificado y cómo se abordan
e) Determinar los requisitos legales y reglamentarios aplicables y otros requisitos relevantes para las actividades, procesos, productos y servicios del auditado

Establecer Contacto con el Auditado

f) Confirmar el acuerdo con el auditado sobre el alcance de la divulgación y el tratamiento de la información confidencial
g) Hacer arreglos para la auditoría incluyendo el cronograma
h) Determinar los arreglos específicos de ubicación para el acceso, la salud y la seguridad, la confidencialidad u otros
i) Acordar la asistencia de los observadores y la necesidad de guías o intérpretes para el equipo de auditoría
j) Determinar cualquier área de interés, preocupación o riesgo para el auditado en relación con la auditoría específica
k) Resolver problemas relacionados con la composición del equipo de auditoría con el auditado o el cliente de auditoría

Determinación de la Viabilidad de la Auditoría

La determinación de la viabilidad debería tener en cuenta factores como la disponibilidad de lo siguiente:

a) Información suficiente y apropiada para planificar y llevar a cabo la auditoría
b) Cooperación adecuada del auditado
c) Tiempo y recursos adecuados para realizar la auditoría

Realizar Revisión de Información Documentada

Debería revisarse la documentación para:

- Recopilar información para comprender las operaciones del auditado y preparar las actividades de auditoría y los documentos de trabajo de auditoría aplicables (ver 6.3.4), por ejemplo; en procesos y funciones
- Establecer una visión general del alcance de la información documentada para determinar la posible conformidad con los criterios de auditoría y detectar posibles áreas de preocupación, como deficiencias, omisiones o conflictos

La información documentada debería incluir, pero no limitarse a:

- Documentos y registros del sistema de gestión
- Informes de auditoría anteriores

La revisión debería tener en cuenta el contexto de la organización del auditado, incluidos su tamaño, naturaleza y complejidad, y sus riesgos y oportunidades relacionados. También debería tener en cuenta el alcance, los criterios y los objetivos de la auditoría.

Planificación de Auditoría

Enfoque basado en el riesgo para la planificación

El líder del equipo de auditoría debería adoptar un enfoque basado en el riesgo para planificar la auditoría con base en la información del programa de auditoría y la información documentada proporcionada por el auditado.

Al planificar la auditoría, el líder del equipo auditor debería considerar lo siguiente:

a) La composición del equipo de auditoría y su competencia general
b) Las técnicas de muestreo apropiadas
c) Oportunidades para mejorar la efectividad y eficiencia de las actividades de auditoría
d) Los riesgos para lograr los objetivos de auditoría creados por una planificación de auditoría ineficaz
e) Los riesgos para el auditado creados al realizar la auditoría

Planificación de Auditoría

Detalles de planificación de auditoría

La planificación de la auditoría debería abordar o hacer referencia a lo siguiente:

a) Los objetivos de la auditoría
b) El alcance de la auditoría, incluida la identificación de la organización y sus funciones, así como los procesos a auditar
c) Los criterios de auditoría y cualquier información documentada de referencia
d) Las ubicaciones (físicas y virtuales), las fechas, el tiempo previsto y la duración de las actividades de auditoría que se llevarán a cabo, incluidas las reuniones con la administración del auditado

Planificación de Auditoría

e) La necesidad de que el equipo de auditoría se familiarice con las instalaciones y los procesos del auditado (por ejemplo, realizando un recorrido por la (s) ubicación (es) física (s), o revisando la tecnología de información y comunicación)
f) Los métodos de auditoría que se utilizarán, incluido el grado en que el muestreo de auditoría es necesario para obtener suficiente evidencia de auditoría
g) Las funciones y responsabilidades de los miembros del equipo de auditoría, así como guías y observadores o intérpretes
h) La asignación de recursos apropiados en base a la consideración de los riesgos y oportunidades relacionados con las actividades que se auditarán

Planificación de Auditoría

La planificación de la auditoría debería tener en cuenta, según corresponda:

- Identificación del (los) representante (s) del auditado para la auditoría
- El lenguaje de trabajo y de informes de la auditoría cuando esto es diferente del lenguaje del auditor o el auditado o ambos
- Los temas del informe de auditoría
- Arreglos de logística y comunicaciones, incluidos arreglos específicos para las ubicaciones que se auditarán
- Cualquier acción específica que se tome para abordar los riesgos para alcanzar los objetivos de auditoría y las oportunidades que surjan
- Cuestiones relacionadas con la confidencialidad y la seguridad de la información
- Cualquier acción de seguimiento de una auditoría anterior u otra (s) fuente (es), por ejemplo:
  - Lecciones aprendidas, revisiones de proyectos
  - Cualquier actividad de seguimiento de la auditoría planificada
  - Coordinación con otras actividades de auditoría, en caso de una auditoría conjunta

Planificación de Auditoría

El plan de auditoría debería incluir:

1. Los objetivos de la auditoría
2. El alcance de la auditoría
3. Los criterios de la auditoría
4. Ubicación, las fechas, el horario y la duración incluyendo las reuniones con la dirección del auditado
5. Las funciones y responsabilidades de los miembros del equipo auditor, así como los guías y observadores
6. La asignación de los recursos necesarios
7. La identificación del representante del auditado
8. El idioma

El plan de auditoría puede ser revisado y aceptado por el cliente de la auditoría y debería presentarse al auditado.

Taller 1

- **Elaborar Plan de Auditoría**

Taller 2

- **Matriz de Plan de Auditoría**

Asignación de Tareas al Equipo Auditor

El líder del equipo auditor, consultando con el equipo auditor, asigna a cada miembro del equipo responsabilidad para:

- Auditar procesos
- Actividades
- Funciones
- Lugares específicos

Las asignaciones deberían considerar la necesidad de:

- Independencia y competencia de los auditores
- El uso eficaz de los recursos
- Diferentes funciones y responsabilidades de los auditores, auditores en formación y expertos técnicos

Funciones y Responsabilidades de Guías y Observadores

Los guías y observadores pueden acompañar al equipo de auditoría con las aprobaciones del líder del equipo de auditoría, el cliente de auditoría y/o el auditado, de ser necesario.

No deberían influir ni interferir en la realización de la auditoría. Si esto no puede garantizarse, el líder del equipo auditor debería tener el derecho de negar la presencia de observadores durante ciertas actividades de auditoría.

Funciones y Responsabilidades de Guías y Observadores

Para los Guías sus responsabilidades deberían incluir lo siguiente:

a) Ayudar a los auditores a identificar a los individuos para que participen en las entrevistas y confirmen los horarios y las ubicaciones
b) Organizar el acceso a ubicaciones específicas del auditado.
c) Garantizar que los miembros del equipo de auditoría y los observadores conozcan y respeten las normas relativas a los acuerdos específicos de localización para el acceso, la salud y la seguridad, el medio ambiente, la seguridad, la confidencialidad y otros asuntos, y que se aborden los riesgos
d) Ser testigo de la auditoría en nombre del auditado, cuando corresponda
e) Proporcionar aclaraciones o ayudar a recopilar información, cuando sea necesario

Preparación de los Documentos de Trabajos

Los miembros del equipo auditor deben recopilar y revisar la información pertinente a las tareas asignadas y preparar los documentos de trabajo, según sea necesario, para referencia y registro de evidencias de la auditoría.

Posibles Ventajas de las Listas de Verificación

a) Aseguran que nada importante se pase por alto
b) Ayudan a brindar continuidad a la auditoría
c) Ayudan a planificar una auditoría eficaz
d) Ayudan a identificar los aspectos más críticos del sistema
e) Ayudan a controlar la profundidad, continuidad y ritmo de la auditoría
f) Registran los hallazgos positivos y negativos
g) Pueden proporcionar un registro de oportunidades de mejora
h) Las listas de verificación previamente confeccionadas pueden inhibir a los auditores
i) Los auditores pueden pasar por alto cuestiones importantes por no estar incluidas en las listas de verificación

Uso de las Listas de Verificación

a) Considerar las listas de verificación como un ayuda memoria
b) Evitar sentirse inhibidos por ellas
c) Escribir prolijamente: la lista de verificación es parte del informe de auditoría
d) Registrar conclusiones finales
e) Registrar oportunidades de mejora
f) Registrar identidades específicas de las muestras examinadas

Taller 3

- **Elaborar una lista de verificación para auditar las clausulas señaladas por el instructor**

Reunión de Apertura

PROPÓSITO:

a) Confirmar el acuerdo de todos los participantes (por ejemplo, auditado, equipo de auditoría) con el plan de auditoría
b) Presentar al equipo de auditoría y sus roles
c) Garantizar que se puedan realizar todas las actividades de auditoría planificadas

Reunión de Apertura

PUNTOS A CONSIDERAR:

- Los objetivos, el alcance y los criterios de la auditoría
- El plan de auditoría y otros arreglos relevantes con el auditado, como la fecha y hora de la reunión de cierre, cualquier reunión interina entre el equipo de auditoría y la administración del auditado, y cualquier cambio necesario
- Canales de comunicación formales entre el equipo de auditoría y el auditado
- El idioma que se utilizará durante la auditoría
- El auditado debería mantenerse informado del progreso de la auditoría durante la auditoría
- La disponibilidad de los recursos y las instalaciones que necesita el equipo de auditoría
- Cuestiones relacionadas con la confidencialidad y la seguridad de la información
- Acceso relevante, salud y seguridad, seguridad, emergencia y otros arreglos para el equipo de auditoría
- Actividades en el sitio que pueden afectar la realización de la auditoría

Reunión de Apertura

PUNTOS A CONSIDERAR:

La presentación de información sobre los siguientes elementos se debería considerar, según corresponda:

- El método de informar los hallazgos de la auditoría, incluidos los criterios para la calificación, si corresponde
- Condiciones bajo las cuales puede darse por terminada la auditoría
- Cómo tratar con posibles hallazgos durante la auditoría
- Cualquier sistema de retroalimentación del auditado sobre los hallazgos o conclusiones de la auditoría, incluidas las quejas o apelaciones

Revisión de la Documentación en la Auditoría

La información documentada relevante del auditado debería ser revisada para:

- Determinar la conformidad del sistema, en la medida documentada, con los criterios de auditoría
- Recopilar información para apoyar las actividades de auditoría

La revisión se puede combinar con las otras actividades de auditoría y puede continuar a lo largo de la auditoría, siempre que esto no sea perjudicial para la efectividad de la realización de la auditoría.

Si no se puede proporcionar la información documentada adecuada dentro del marco de tiempo dado en el plan de auditoría, el líder del equipo de auditoría debería informar tanto a la (s) persona (s) que gestionan el programa de auditoría como al auditado. Dependiendo de los objetivos y el alcance de la auditoría, se debería tomar una decisión sobre si la auditoría debería continuar o suspenderse hasta que se resuelvan los problemas de información documentada.

Comunicación Durante la Auditoría

Durante la auditoría, puede ser necesario hacer arreglos formales para la comunicación dentro del equipo de auditoría, así como con el auditado, el cliente de auditoría y potencialmente con partes interesadas externas (por ejemplo, reguladores), especialmente cuando los requisitos legales y reglamentarios requieren la notificación obligatoria de incumplimiento.

- El equipo de auditoría debería consultar periódicamente para intercambiar información, evaluar el progreso de la auditoría y reasignar el trabajo entre los miembros del equipo de auditoría, según sea necesario
- Durante la auditoría, el líder del equipo de auditoría debe comunicar periódicamente el avance de la auditoría y cualquier inquietud al auditado
- Cuando los objetivos de la auditoría no sean alcanzables el líder del equipo auditor debería informar de las razones a las partes interesadas para tomar acciones apropiadas
- Las acciones pueden incluir la reconfirmación o la modificación del plan, cambios en los objetivos, alcance o la interrupción de la auditoría
- Los cambios deberían revisarse y aprobarse tanto por el gestor del programa de auditoría como por el auditado

Métodos para Recopilar Información

- Entrevistas
- Observación de actividades o lugares de trabajo
- Revisión de documentos, incluyendo registros
- Registros, tales como reportes de ocurrencias de eventos de seguridad, de mediciones de la eficacia de los controles, actas de reunión, informes de auditoría
- Resúmenes de datos, análisis e indicadores de desempeño de incidentes de seguridad
- Informes de otras fuentes, por ejemplo, datos de entidades reguladoras

Métodos para Recopilar Información

Visión general de un proceso típico, desde la recopilación de información hasta llegar a conclusiones de auditoría.

La Entrevista

a) Las entrevistas deben realizarse con personas de niveles apropiados y funciones que realizan actividades o tareas dentro del alcance de la auditoría
b) Las entrevistas deben realizarse durante el horario laboral normal y, donde sea práctico, en lugar de trabajo normal de la persona que se está entrevistado
c) Se debe tratar que la persona que se entrevista esté cómoda antes y durante la entrevista
d) Se debe explicar la razón para la entrevista y cualquier nota que se tome
e) Se deben resumir y revisar los resultados de la entrevista con la persona entrevistada
f) Se debe agradecer a las personas entrevistadas por su participación y cooperación

Preguntas Claves del Auditor

Tipo de Preguntas

- ¿Realizaron auditorías internas?
- ¿Existe una política del Sistema de Gestión?
- ¿El Sistema de Gestión ha sido comunicado?
- ¿Es usted parte del grupo auditor interno?
- ¿El proceso se ejecuta como está documentado?
- ¿En dónde registra la información?
- ¿Cuál procedimiento?
- ¿Conoce la política?
- ¿Cumple la legislación?

Ejecutando la Auditoría

- Haga un muestreo de actividades, no se centre en una
- Busque evidencia observando lo que ocurre y revisando registros
- Haga anotaciones completas
- Escuche las explicaciones del auditado
- Anote y confirme los hallazgos u observaciones. Si tiene dudas sobre el cumplimiento de un requisito podría hacer algunas preguntas abiertas adicionales
- Siempre escriba los detalles de lo observado o evidenciado, por ejemplo, debería anotar el procedimiento auditado, los identificadores de los registros, numero de órdenes, identificación de lotes, códigos de documentos etc
- Auditoría abierta y amigable resultará en un acuerdo de que el problema existe
- Verifique si la No Conformidad es o no puntual

Realización de Entrevistas

- Sea amigable
- Haga sentir cómodo al auditado
- Explicar las razones de la entrevista y de las notas tomadas
- Iniciar con una descripción de las actividades
- No realizar preguntas inductivas (Evita preguntas cuya respuesta sea SI o NO)
- Agradecer a los auditados

Administración del Tiempo

- Realizar primero las actividades más complejas o difíciles
- Asignar trabajo a los otros auditores
- Adquirir el hábito de hacerlo de inmediato
- Conocer curva de cansancio del auditado y auditor
- Establecer limite de tiempo y cumplirlo
- Ser creativo

Manejo de Situaciones Difíciles

- A la reunión de apertura no se presenta el responsable del proceso o actividad auditada
- En la auditoría se tenía previsto visitar dos instalaciones y no hay disponibles vehículos, ni acompañantes
- El auditado desvía la pregunta del auditor. Ejemplo: pregunta por la forma como se controlan los documentos y el auditado explica la forma como se controlan los registros, dado que los documentos son un tipo de registro
- El auditado suministra poca información. Ejemplo: se solicita información sobre los resultados de enero a mayo y solo presenta los resultados del último mes
- El auditado reformula las preguntas del auditor
- El auditado cuestiona las preguntas del auditor. Ejemplo: lo que usted pregunta no tiene sentido
- En la reunión de apertura no hay acuerdo con el objeto y alcance de la auditoría

Resultados de la Auditoría

Hallazgo

- Resultados de la evaluación de la evidencia objetiva recopilada frente al conjunto de políticas, procedimientos o requisitos utilizados como referencia
- Es registrado en la lista de verificación como respuesta a los cuestionamientos que han sido preparados

Tipos de Hallazgos

- **No conformidad**: Incumplimiento de un requisito especificado
- **Observación:** Situación que potencialmente puede afectar el sistema de gestión de calidad

Incumplimientos Más Comunes

- Documentación no encontrada
- Competencias de recurso humano no evaluada
- Controles implementados inadecuados
- No conformidades por auditorías internas sin cierre eficaz
- Acciones correctivas sin revisión de la dirección
- Deficiencia en metodología de análisis de riesgo
- Incumplimiento de procedimientos

Redacción de las No Conformidades

- **La Evidencia**: Lista de hallazgos, respaldados con evidencias objetivas o atestiguadas por el auditado
- **La Referencia**: Al requisito de la norma y/o manual de calidad o procedimiento. Un requisito a la vez, el que más aplica
- **La Conclusión**: Genérica, breve, precisa y aceptada por el auditado
- **No Conformidad:** Incumplimiento a un requisito de la Norma auditada
- **Observación:** Hallazgo detectado en Auditoría que podría generar una no conformidad si no es tratado
- **Oportunidad de Mejora:** Son situaciones que no representan incumplimiento, pero pueden ser revisadas por la organización, cuando lo estime conveniente para mejorar la eficacia del proceso

Fórmula de Redacción de No Conformidades

Reporte debe contener como mínimo:

- Una visión general del hallazgo
- Descripción completa y precisa de lo observado
- Ejemplos de la evidencia de auditoría
- Referencia a la cláusula del estándar/documento de la organización
- Explicación de los requisitos de la cláusula/documento
- Las discrepancias deben atribuirse solamente a una cláusula de la norma, la más aplicable
- En ocasiones, la única referencia es la documentación de la organización

Conclusiones de Auditoría

El equipo auditor debe reunirse antes de la “reunión de cierre” para:

- Revisar los hallazgos de la auditoría y cualquier otra información apropiada recopilada durante la auditoría frente a los objetivos de la misma
- Acordar conclusiones de auditoría
- Preparar recomendaciones, si así lo especifica el plan de auditoría

Las conclusiones de auditoría pueden tratar aspectos como:

- Evaluación del grado de cumplimiento con el criterio de auditoría
- Eficacia de la implementación, mantenimiento y mejoras del sistema de gestión
- Capacidad del proceso de revisión por la dirección para asegurar la adecuación, eficacia y mejora sostenida del SGSI

Informe de Auditoría

Debería contener:

- Objetivos de la auditoría
- Alcance de la auditoría, particularmente la definición de las unidades de la organización o de los procesos auditados y el período de la auditoría
- Documentación de la persona de contacto
- Documentación del auditor líder y otros auditores
- Fechas y ubicaciones donde se desarrollaron las actividades de la auditoría
- Criterio de auditoría
- Declaraciones de auditoría
- Conclusiones de la auditoría

Reunión de Cierre

Es facilitada por el auditor líder. Según corresponda, lo siguiente debería explicarse al auditado en la reunión de clausura:

a) Informar que la evidencia de auditoría recopilada se basó en una muestra de la información disponible y no es necesariamente representativa de la eficacia general de los procesos del auditado
b) El método de informar
c) Cómo debería abordarse la conclusión de la auditoría en función del proceso acordado
d) Posibles consecuencias de no abordar adecuadamente los hallazgos de la auditoría
e) Presentación de los hallazgos y conclusiones de auditoría de tal manera que la gerencia del auditado los comprenda y los reconozca
f) Cualquier actividad posterior a la auditoría relacionada (por ejemplo, implementación y revisión de acciones correctivas, tratamiento de quejas de auditoría, proceso de apelación)

Preparación y Distribución del Informe de Auditoría

El líder del equipo auditor debería informar las conclusiones de la auditoría de acuerdo con el programa de auditoría.

El informe de auditoría debería proporcionar un registro completo, preciso, conciso y claro de la auditoría, e incluir o hacer referencia a lo siguiente:

a) Objetivos de auditoría
b) Alcance de la auditoría, particularmente identificación de la organización (el auditado) y las funciones o procesos auditados
c) Identificación del cliente de auditoría
d) Identificación del equipo de auditoría y los participantes del auditado en la auditoría

Preparación y Distribución del Informe de Auditoría

e) Fechas y lugares donde se llevaron a cabo las actividades de auditoría
f) Criterios de auditoría
g) Hallazgos de auditoría y evidencia relacionada
h) Conclusiones de auditoría
i) Una declaración sobre el grado en que se han cumplido los criterios de auditoría
j) Cualquier opinión divergente no resuelta entre el equipo de auditoría y el auditado
k) Las auditorías por naturaleza son un ejercicio de muestreo; como tal, existe el riesgo de que la evidencia de auditoría examinada no sea representativa

Preparación y Distribución del Informe de Auditoría

El informe de auditoría debería emitirse dentro del tiempo acordado. Si se retrasa, los motivos deberían comunicarse al auditado y a la (s) persona (s) que gestionan el programa de auditoría.

El informe de auditoría debería estar fechado, revisado y aceptado, según corresponda, de conformidad con el programa de auditoría.

El informe de auditoría debería distribuirse a las partes interesadas pertinentes definidas en el programa de auditoría o el plan de auditoría.

Al distribuir el informe de auditoría, se deberían considerar medidas apropiadas para garantizar la confidencialidad.

Preparación y Distribución del Informe de Auditoría

La auditoría se completa cuando se han llevado a cabo todas las actividades de auditoría planificadas, o según se acuerde con el cliente de auditoría (por ejemplo, puede haber una situación inesperada que impida completar la auditoría de acuerdo con el plan de auditoría).

La información documentada relativa a la auditoría debería conservarse o eliminarse por acuerdo entre las personas participantes y de acuerdo con el programa de auditoría y los requisitos aplicables.

A menos que lo exija la ley, el equipo de auditoría y las personas que gestionan el programa de auditoría no deberían divulgar ninguna información obtenida durante la auditoría, o el informe de auditoría, a ninguna otra parte sin la aprobación explícita del cliente de auditoría y, cuando corresponda, la aprobación del auditado.

Las lecciones aprendidas de la auditoría pueden identificar riesgos y oportunidades para el programa de auditoría y el auditado.

Realización de Seguimiento de Auditoría

- El resultado de la auditoría puede, dependiendo de los objetivos de la auditoría, indicar la necesidad de correcciones o de acciones correctivas u oportunidades de mejora. Tales acciones generalmente son decididas y llevadas a cabo por el auditado dentro de un plazo acordado. Según corresponda, el auditado debería mantener informadas a las personas que gestionan el programa de auditoría y/o al equipo de auditoría sobre el estado de estas acciones
- La finalización y efectividad de estas acciones debería ser verificada. Esta verificación puede ser parte de una auditoría posterior. Los resultados se deberían informar a la persona que gestiona el programa de auditoría y se informa al cliente de auditoría para su revisión por la dirección

Las Auditorías de Seguimiento

Responsabilidades del auditor:

- Acordar la fecha de la auditoría de seguimiento
- Desarrollar la auditoría de seguimiento de acuerdo con las acciones correctivas y preventivas
- Presentar e informar los resultados de la auditoría de seguimiento
- Evaluar la eficacia de las acciones correctivas y preventivas implantadas

Taller 4

- **Según el formato, realizar el informe de auditoría**

Conclusiones

Conclusiones

La Normal ISO 27001 puede ser implementada en cualquier tipo de organización pues proporciona una metodología para implementar un Sistema para la Gestión de la Seguridad de la Información, permitiendo también que una empresa sea certificada según el cumplimiento de esta norma, donde su eje central es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde se encuentran, para así tratarlos sistemáticamente.

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#ISO27001 IA-LA #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com