certiprof®

ISO 27001 FOUNDATION

PROFESSIONAL CERTIFICATION

I27001F™ Versión 112022

ISO 27001 FOUNDATION
I27001F

I27001F™ Versión 112022

¿Quién es Certiprof®?

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

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

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

Nuestras Afiliaciones

Memberships

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**

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:**

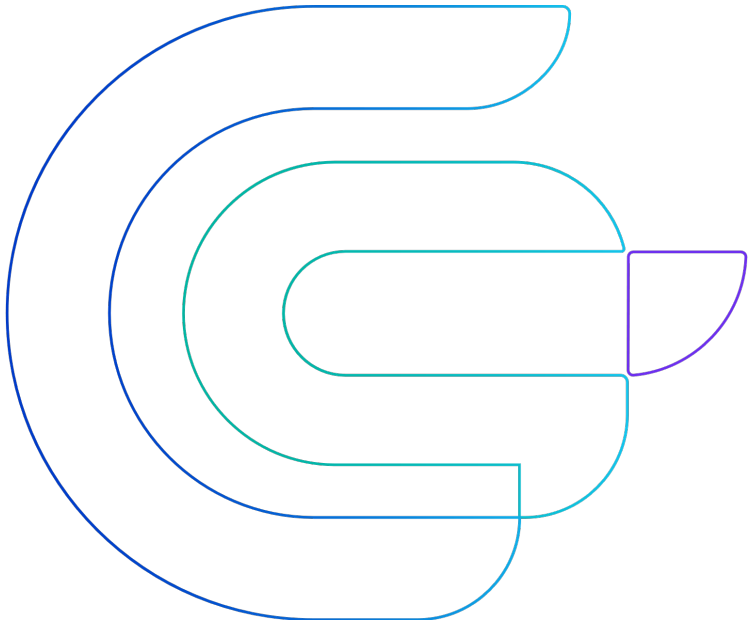
  Un estudio de la **Asociación Internacional de Gestión de Proyectos (PMI)** encontró que los candidatos que muestran insignias digitales de gestión de proyectos tienen **un 60%** más de probabilidades de ser contratados en comparación con aquellos que solo mencionan sus habilidades sin verificación digital.

¿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

Certified ISO 27001 Foundation - I27001F

Issued by Certiprof

Holders of this certification have demonstrated an understanding of the Principles, concepts and the requirements of ISO/IEC 27001:2022, its understanding and how it can be used. They know the fundamental requirements for the implementation of an ISMS and the great importance of maintaining continuous process improvement.

Learn more

Earn this Badge

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-foundation-i27001f.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

COMPARTE Y VERIFICA TUS LOGROS DE APRENDIZAJE FÁCILMENTE

#I27001F #certiprof

certiprof®

Agenda

Agenda

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.

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

1. Introducción y Antecedentes

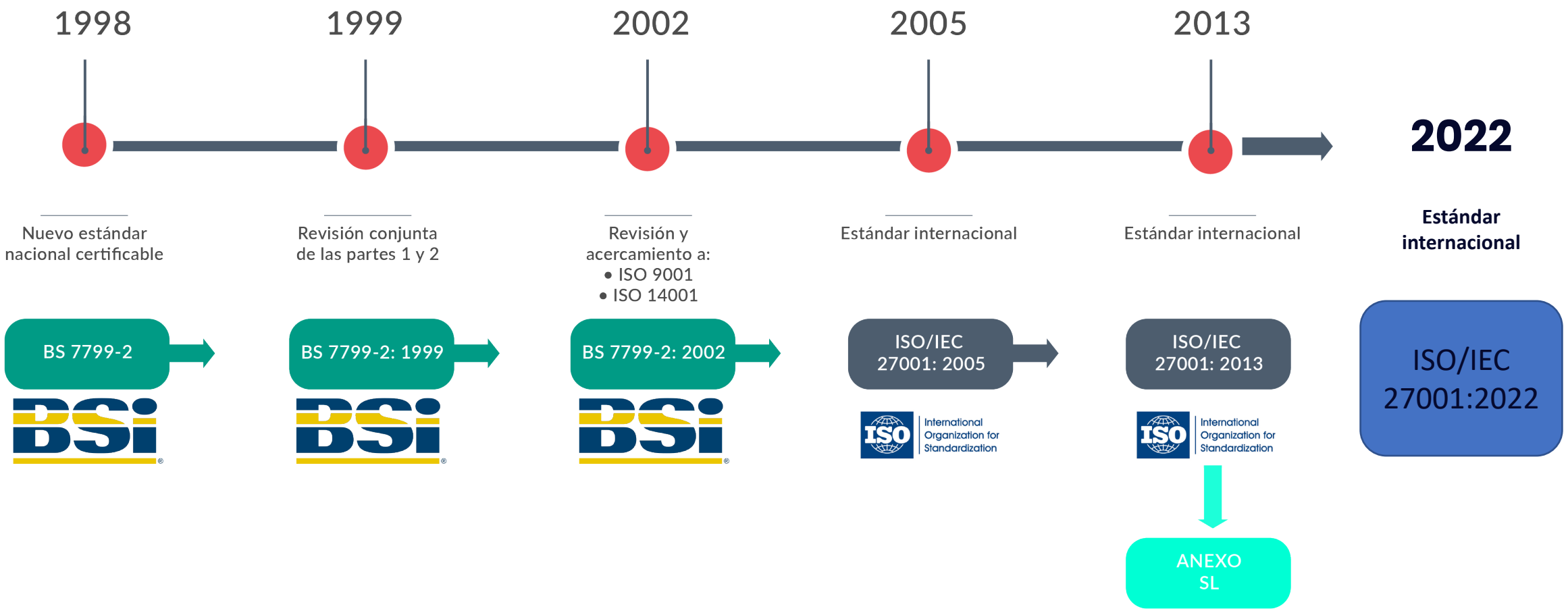
Introducción

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

Introducción

- La Norma ha sido diseñada para ***"proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información"***.
- La Norma ***"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"***.
- La Norma también incluye ***"requisitos para la evaluación y el tratamiento de los riesgos en la seguridad de la información a la medida de las necesidades de la organización. 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"***.

Historia de la Norma



ISO/IEC 27001:2022 Estructura

La nueva estructura refleja la estructura de otras normas nuevas de gestión, tales como ISO 9000, ISO 20000 e ISO 22301, que ayudan a las organizaciones a cumplir con varias normas.

Los cambios que se presentaron en la industria con la aparición del Marco de Ciberseguridad del NIST (CSF) cuyo enfoque era proteger la infraestructura crítica que soporta los servicios esenciales de los Estados Unidos, las propuestas de Ciberseguridad de la Unión Europea reflejados en diversos documentos de la ENISA y las actualizaciones que ocurrieron en otras mejores prácticas como ITIL y COBIT -durante 2019- y PCI, durante este año también han influido en la necesidad de refrescar el contenido de esta norma.

Hay 93 controles en 4 grupos en comparación con los 114 controles en 14 cláusulas en la versión de 2013.

ISO/IEC 27001:2022 Estructura

Seguridad de la información, ciberseguridad y protección de la privacidad, sistemas de gestión de la seguridad de la información y requisitos.

Se agregaron 11 nuevos controles (Inteligencia de amenazas, Seguridad de la información en la nube, continuidad del negocio, seguridad física y su supervisión, configuración, eliminación de la información, encriptación de datos, seguimiento y monitoreo, filtrado web, codificación segura)

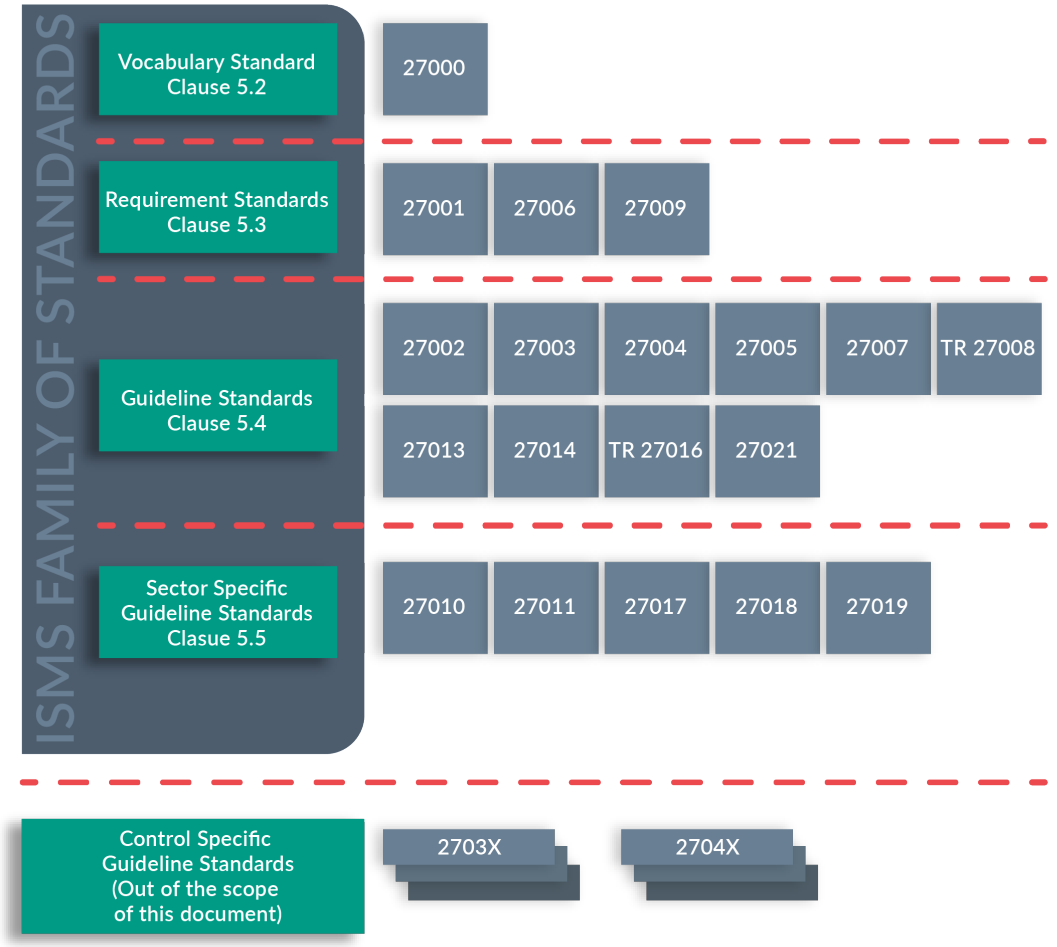
1 control se eliminó (eliminación de activos)
58 controles se actualizaron
24 controles fusionados
4 grupos o tipos de controles: organizacional (37 controles), personas (8 controles), físico (14 controles), tecnológico (34 controles)

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?

I27001F™ Versión 112022

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, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos.

El análisis de los requisitos para la protección de los activos de la información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un **SGSI**.

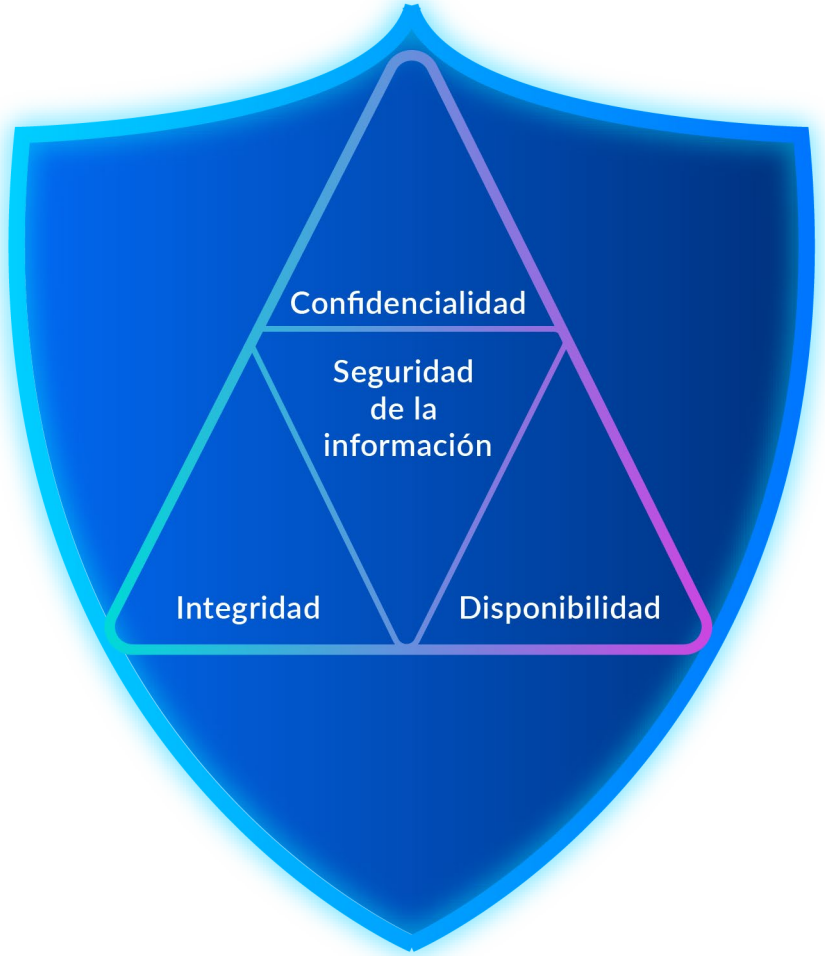
Información y Principios Generales

Los siguientes principios fundamentales también pueden contribuir a la implementación exitosa de un **SGSI**:

a) La conciencia de la necesidad de seguridad de la información.
b) La asignación de responsabilidades en seguridad de la información.
c) La incorporación del compromiso de la Dirección y los intereses de las partes interesadas.
d) La mejora de los valores sociales.
e) Apreciaciones de riesgo para determinar los controles adecuados para alcanzar niveles aceptables de riesgo.
f) La seguridad incorporada como un elemento esencial de los sistemas y redes de información.
g) La prevención y detección activas de incidentes de seguridad de la información.
h) El garantizar una aproximación exhaustiva a la gestión de la seguridad de la información.
i) La evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

La Seguridad de la Información

La seguridad de la información incluye tres dimensiones principales: **la confidencialidad**, **la disponibilidad** y **la integridad**. Con el objetivo de garantizar el éxito empresarial sostenido, así como su continuidad y minimizar impactos, la seguridad de la información conlleva la aplicación y la gestión de medidas de seguridad adecuadas, que implican la consideración de una amplia gama de amenazas.



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

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 son principalmente la reducción de los riesgos asociados a la seguridad de la información (es decir, reduciendo la probabilidad y/o el impacto causado por los incidentes de seguridad de la información). De una forma más específica los beneficios que para una organización produce la adopción exitosa de la familia de normas **SGSI** son:

a) Un apoyo al proceso de especificar, implementar, operar y mantener un **SGSI**, global, eficiente en costes, integrado y alineado que satisfaga las necesidades de la organización en diferentes operaciones y lugares.
b) Una ayuda para la dirección en la estructura de su enfoque hacia la gestión de la seguridad de la información, en el contexto de la gestión y gobierno del riesgo corporativo, incluidas las acciones de educación y formación en una gestión holística de la seguridad de la información a los propietarios del negocio y del sistema.

Beneficios de la Familia de Normas SGSI

c) La promoción de buenas prácticas de seguridad de la información, aceptadas a nivel mundial, de una manera no preceptiva, dando a las organizaciones la flexibilidad para adoptar y mejorar los controles aplicables, respetando sus circunstancias específicas y para mantenerlos de cara a futuros cambios internos y externos.

d) Disponer de un lenguaje común y una base conceptual para la seguridad de la información, haciendo más fácil confiar a los socios de un negocio que esté en conforme a un **SGSI**, especialmente si requieren la certificación conforme a la Norma ISO/IEC 27001 por un organismo de certificación acreditado.

e) Aumentar la confianza en la organización por las partes interesadas.

f) Satisfacer necesidades y expectativas sociales.

g) Una más eficaz gestión desde un punto de vista económico de las inversiones en seguridad de la información.

3. Términos y Definiciones
(Ver anexo)

Estructura de la Norma

Estructura de ISO/IEC 27001

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

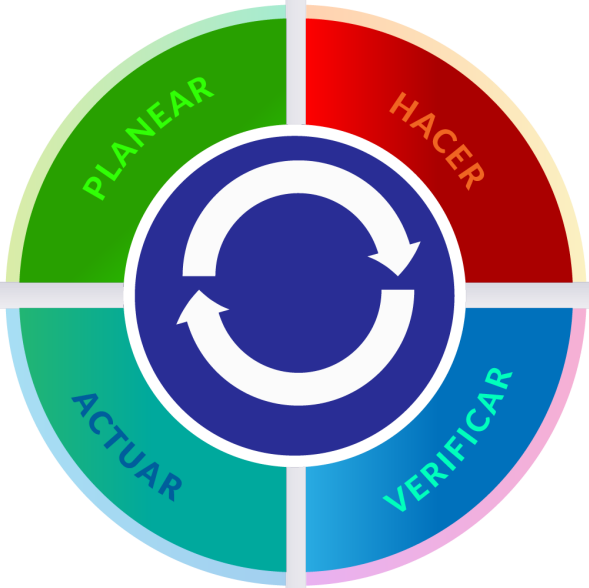
4. Contexto de la organización
5.Liderazgo
6.Planificación
7.Soporte
8.Operación
9.Evaluación del desempeño
10.Mejora

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

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 a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA: La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerando el apartado **5.3** de la Norma ISO 31000.

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.

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 de estas partes interesadas que son relevantes para la 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:

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

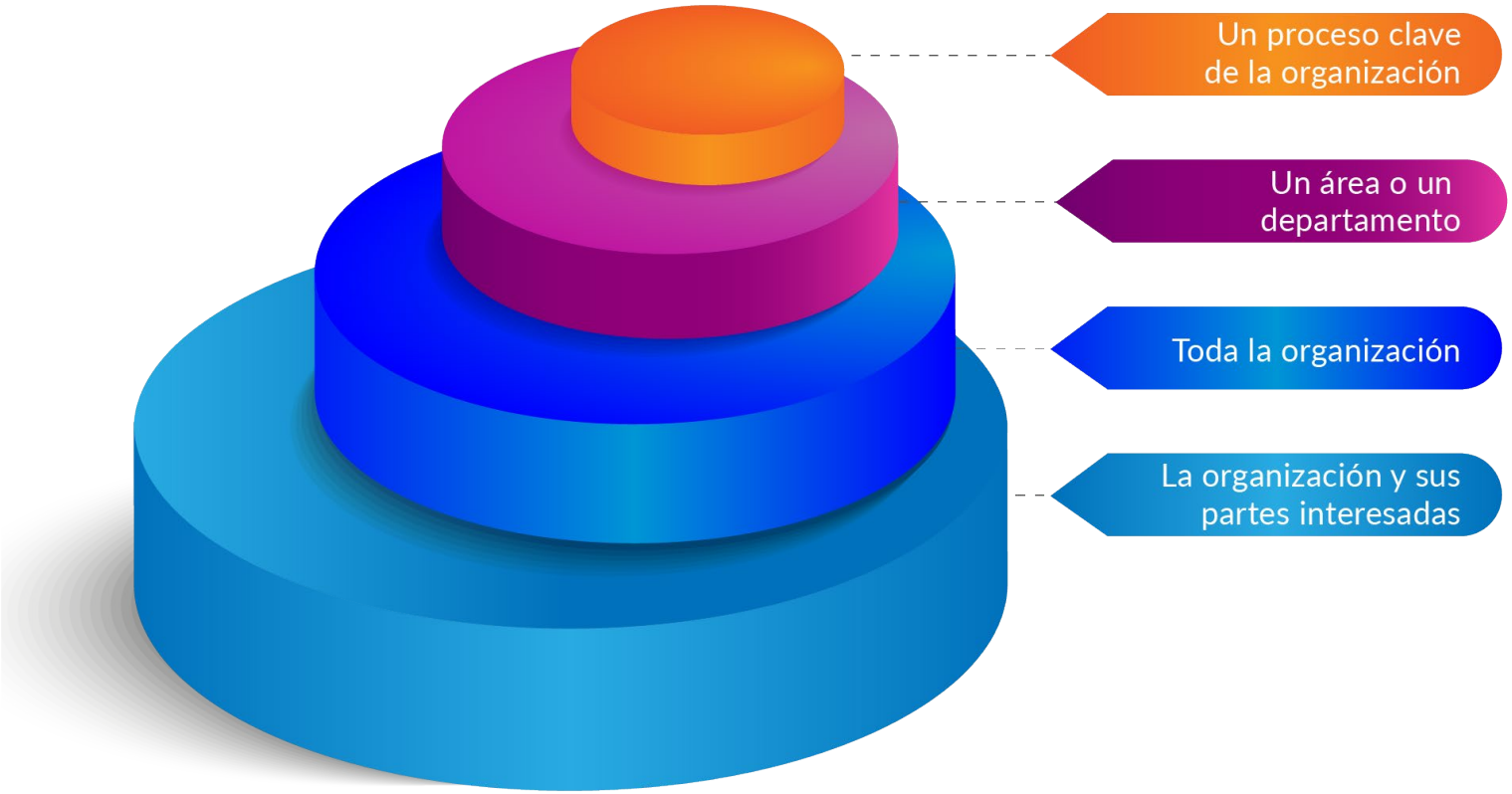
La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

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



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

Para el alcance es relevante tener en cuenta los siguientes aspectos:

- Los resultados del contexto.
- Los resultados del análisis de brechas.
- Los Sistemas de Gestión existentes en la organización.
- Las áreas de aplicación que dan valor a las partes interesadas.
- Los requisitos legales, regulatorios, contractuales.
- Los objetivos de la Organización.
- Los límites organizacionales.
- Los límites de los sistemas de información.
- Los límites físicos.

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:

- Definición del Alcance.
- Características de la organización.
- Procesos de la organización.
- Funciones y responsabilidades.
- Activos de Información.
- Sistemas de Información.
- Ubicación geográfica.

4.4 Sistema de Gestión de la Seguridad de la Información

La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, 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 se establecen la política y los objetivos de seguridad de la información y que estos sean compatibles con la dirección estratégica de la organización

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

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

5.1 Liderazgo y Compromiso

d) Comunicando la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información

e) Asegurando que el sistema de gestión de la seguridad de la información consigue los resultados previstos

f) Dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información

g) Promoviendo la mejora continua

h) Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad

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:

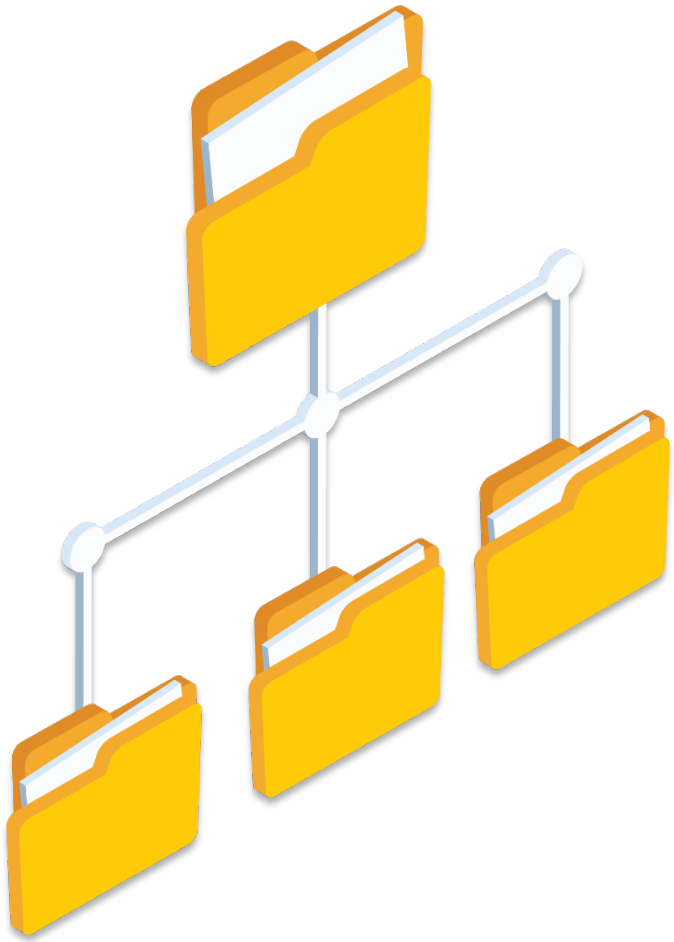
a) Sea adecuada al propósito de la organización

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 cumplir con los requisitos aplicables 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:

a) Estar disponible como información documentada

b) Comunicarse dentro de la organización

c) Estar disponible para las partes interesadas, según sea apropiado

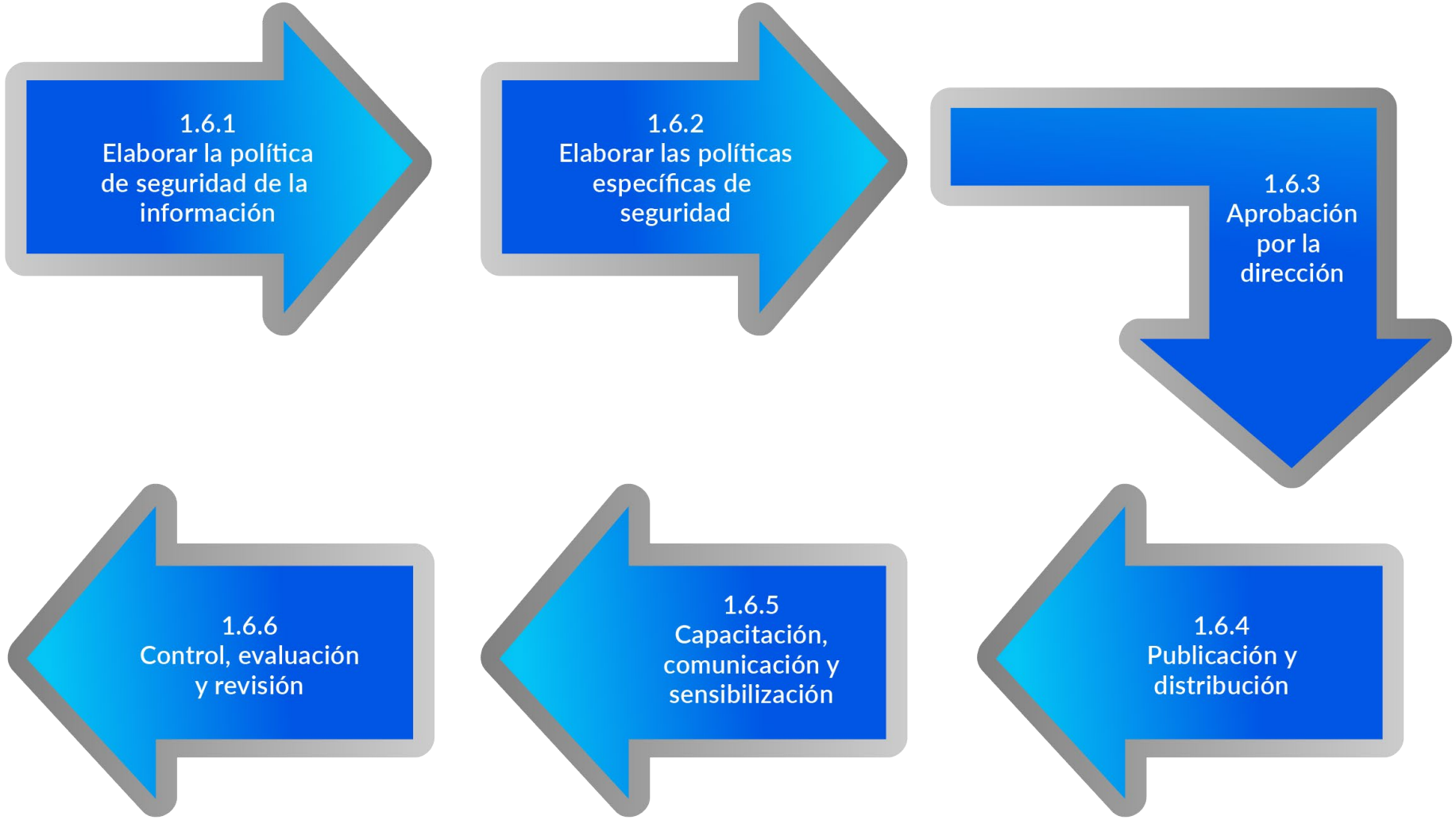
5.2 Política

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 comportamiento 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 se 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 y establecer las autoridades que pueden ser mediante la designación de un Comité SGSI.

Las buenas practicas 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.

Así mismo 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 la seguridad de la información, la organización debe considerar las cuestiones a las que se hace referencia en el apartado **4.1** y los requisitos incluidos en el apartado **4.2**, y determinar los riesgos y oportunidades que es necesario tratar con el fin de:

a) Asegurar que el sistema de gestión de la seguridad de la información pueda conseguir sus resultados previstos

b) Prevenir o reducir efectos indeseados

c) Lograr la mejora continua

6.1 Acciones para Tratar los Riesgos y Oportunidades

La organización debe planificar:

a) Las acciones para tratar estos riesgos y oportunidades
b) La manera 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 Apreciación de Riesgos de Seguridad de la Información

La organización debe definir y aplicar un proceso de apreciación 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 apreciaciones de los riesgos de seguridad de la información
b) Asegure que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables
c) Identifique los riesgos de seguridad de la información:
   1. Llevando a cabo el proceso de apreciación de riesgos de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información
   2. Identificando a los dueños de los riesgos

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

6.1 Acciones para Tratar los Riesgos y Oportunidades

6.1 Acciones para Tratar los Riesgos y Oportunidades

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

- **Propietario del riesgo**: Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo
- **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. Valorando las posibles consecuencias que resultarían si los riesgos identificados en el punto **6.1.2 c) 1)** llegasen a materializarse
   2. Valorando de forma realista la probabilidad de ocurrencia de los riesgos identificados en el punto **6.1.2 c) 1)**
   3. Determinando los niveles de riesgo

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

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

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 1: El anexo A contiene una amplia lista de objetivos de control y controles. 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 2: Los objetivos de control se incluyen implícitamente en los controles seleccionados. Los objetivos de control y los controles enumerados en el 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 dueños de los riesgos

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

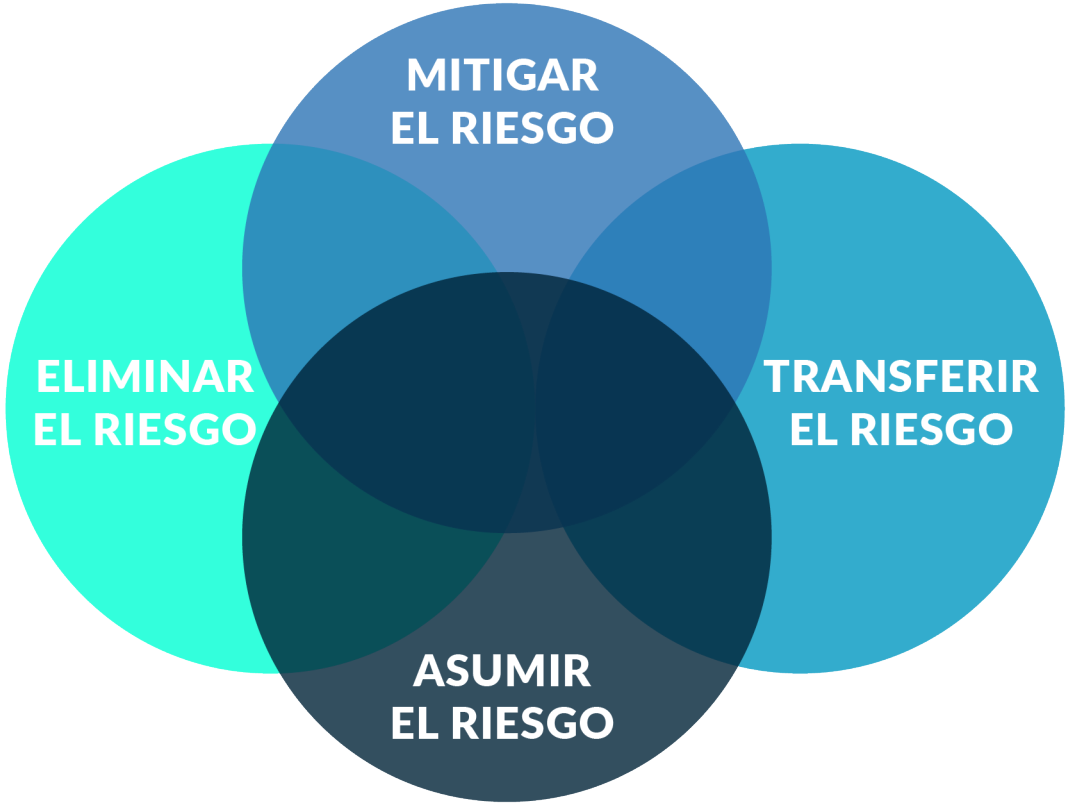
NOTA: La apreciación de los riesgos de seguridad de la información y el proceso de tratamiento recogido en esta norma internacional se alinean con los principios y directrices genéricas definidos en la **Norma ISO 31000**.

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)
- **Eliminar:** 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

Taller (25 minutos)

Definir Declaración de Aplicabilidad para 5 Controles del Anexo A.

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 apreciación y del tratamiento de los riesgos
d) Ser monitoreados
e) Ser comunicados
f) Ser actualizados, según sea apropiado

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

g) 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:

a) Lo que se va a hacer
b) Qué recursos se requerirán
c) Quién será responsable
d) Cuándo se finalizará
e) 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 información
					Entre 6 % y 7%	Regular				
					Mayor o igual a 8%	Malo				

6.3 Planificación de cambios

Cuando la organización lo determine la necesidad de hacer cambios en el SGSI, debe llevarlos a cabo de manera planificada.

Taller (25 minutos)

Definir los Objetivos de Seguridad de la Información.

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

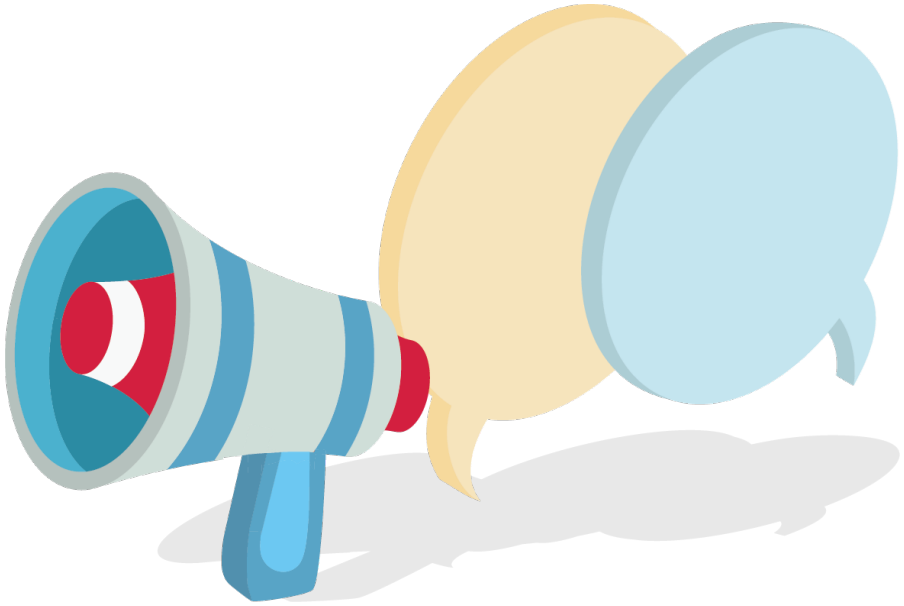
Las personas que trabajan bajo el control de la organización deben ser conscientes de:

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, que incluyan:

a) El contenido de la comunicación
b) Cuándo comunicar
c) A quién comunicar
d) Quién debe comunicar
e) Los procesos por los que debe efectuarse la comunicación

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 eficacia 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

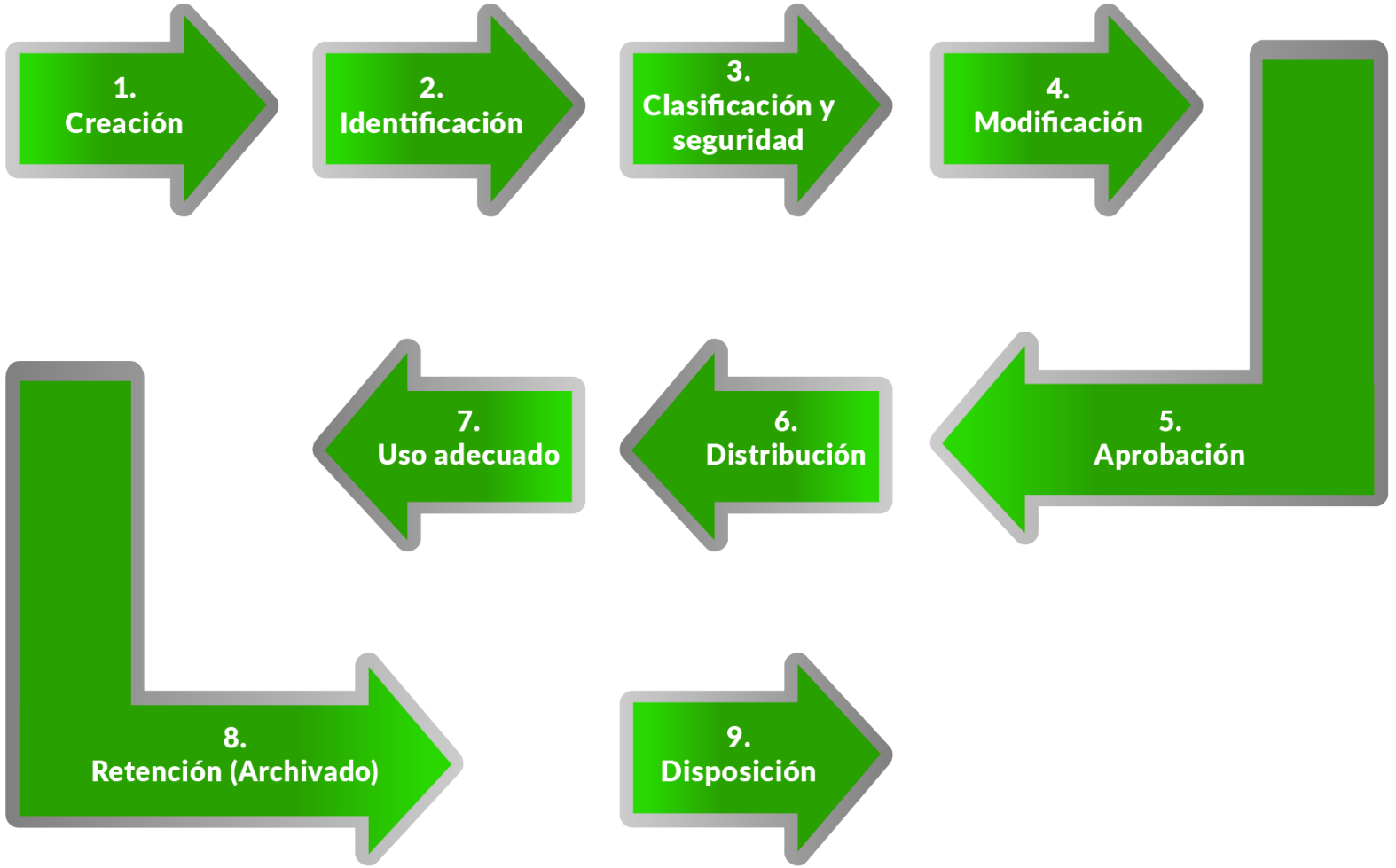
Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

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, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información se debe identificar y controlar, según sea adecuado.

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 los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado **6.1**. La organización debe implementar también planes para alcanzar los objetivos de seguridad de la información determinados en el apartado **6.2**.

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

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

La organización debe garantizar que los procesos contratados externamente estén controlados.

8.2 Apreciación de los Riesgos de Seguridad de la Información

La organización debe efectuar apreciaciones 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

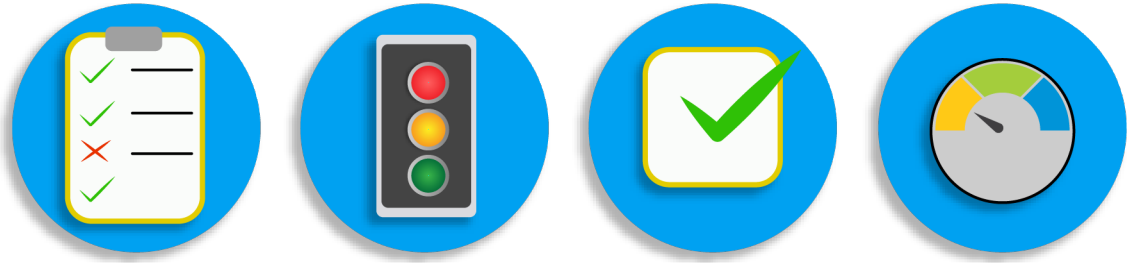
Probabilidad	Impacto: 1 Insignificante	2 Menor	3 Dañino	4 Severo	5 Crítico
1 Raro	B(1)	B(2)	M(3)	M(4)	M(5)
2 Improbable	B(2)	M(4)	M(6)	M(8)	M(10)
3 Posible	M(3)	M(6)	A(9)	A(12)	A(15)
4 Probable	M(4)	M(8)	A(12)	A(16)	E(20)
5 Casi Seguro	M(5)	M(10)	A(15)	A(20)	E(25)

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.

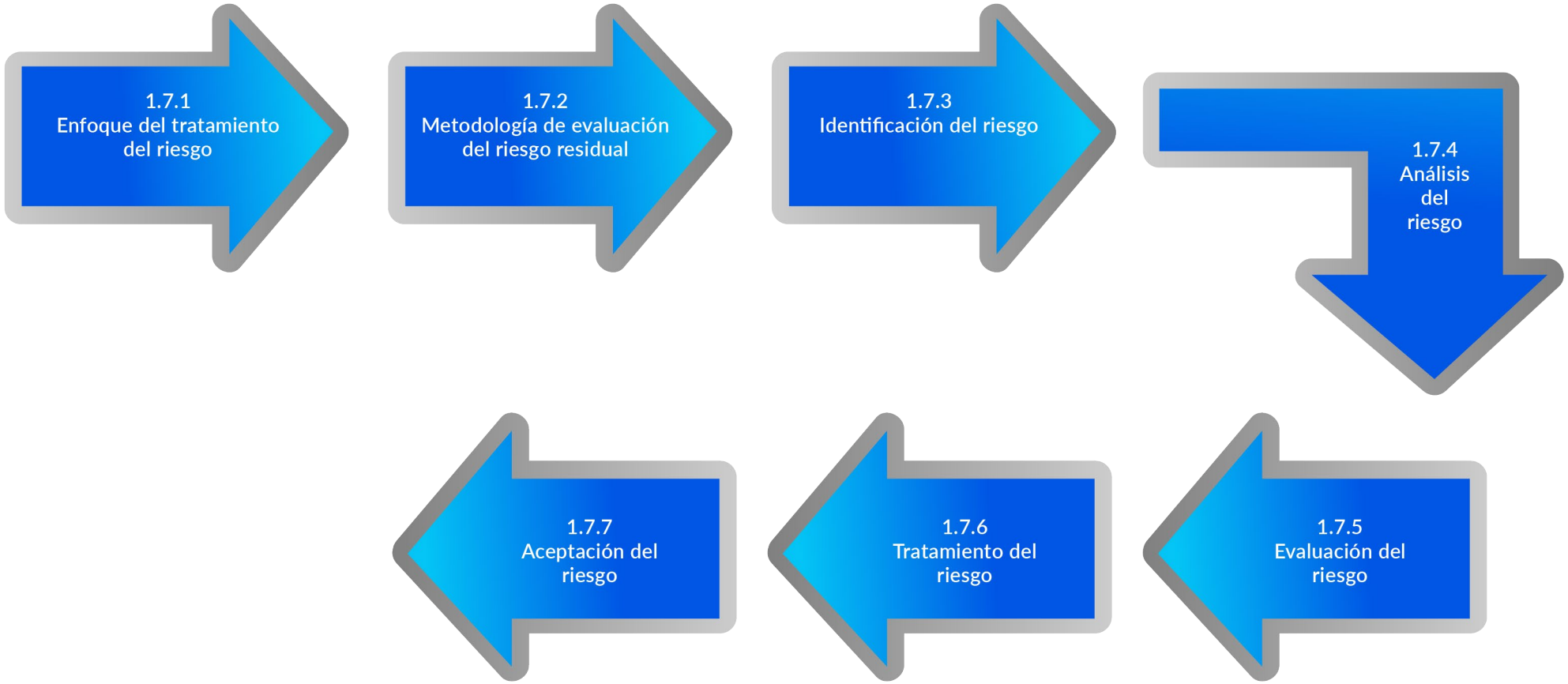
La organización debe conservar información documentada de los resultados del tratamiento de los riesgos de seguridad de la información.



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

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

NOTA: Los métodos seleccionados deben producir resultados comparables y reproducibles para ser considerados válidos.

9.1 Seguimiento, Medición, Análisis y Evaluación

c) Cuándo se deben llevar a cabo el seguimiento y la medición
d) Quién debe hacer el seguimiento y la medición.
e) Cuándo se deben analizar y evaluar los resultados del seguimiento y la medición
f) Quién debe analizar y evaluar esos resultados

La organización debe conservar la información documentada adecuada como evidencia de los resultados.

9.1 Seguimiento, Medición, Análisis y Evaluación

9.2 Auditoría Interna

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) Está implementado y mantenido de manera eficaz

9.2 Auditoría Interna

La organización debe:

a) Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas

b) Para cada auditoría, definir sus criterios y su alcance

c) Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría

d) Asegurarse de que se informa a la dirección pertinente de los resultados de las auditorías

e) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de esta

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

9.3.1 Generalidades: 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 Entrada 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 sean relevantes para el SGSI

d) Resultados del desempeño del SGSI como:

1. No conformidades y acciones correctivas
2. Seguimiento y resultados de las mediciones
3. Resultados de auditoría
4. El cumplimiento de los objetivos de seguridad de la información

9.3 Revisión por la Dirección

e) Retroalimentación de las partes interesadas
f) Los resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos
g) Las oportunidades de mejora continua

9.3.3 Salidas de la Revisión por la Dirección: Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por 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 SGS
3. Los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en: no conformidades y acciones correctivas
4. Resultados del monitoreo y mediciones
5. Resultados de auditoría
6. Cumplimiento de los objetivos de seguridad de la información
7. Comentarios de las partes interesadas
8. Resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo
9. Oportunidades para la mejora continua

10. Mejora

10.1 Mejora continua 10.2 No conformidad y acciones correctivas

10.1. Mejora continua: la organización deben continuamente mejorar la adecuación, sostenimiento y efectividad del SGSI.

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 1: Términos y Definiciones

Taller (25 minutos)

Revisar los Términos y Definiciones de Seguridad de la Información

3.1 Control de Acceso

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

3.2 Modelo Analítico

Algoritmo o cálculo que combina una o más **medidas básicas** (3.10) o **derivadas** (3.22) siguiendo los criterios de decisión asociados a las mismas.

3.3 Ataque

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

3.4 Atributo

Propiedad o característica de un **objeto** (3.55) que es cuantitativa o cualitativamente distinguible por medios humanos o automáticos.

[Adaptada de ISO/IEC 15939:2007]

3.5 Auditoría

Proceso (3.61) sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

NOTA 2: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

3.6 Alcance de la Auditoría

Extensión y límites de una **auditoría** (3.5).

[ISO 19011:2011]

3.7 Autenticación

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

3.8 Autenticidad

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

3.9 Disponibilidad

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

3.10 Medida Básica

Medida (3.47) definida por medio de un **atributo** (3.4) y el método para cuantificarlo.

[ISO/IEC 15939:2007]
NOTA: Una medida básica es funcionalmente independiente de otras medidas.

3.11 Competencia

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

3.12 Confidencialidad

Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o **procesos** (3.61) no autorizados.

3.13 Conformidad

Cumplimiento de un **requisito** (3.63).

3.14 Consecuencia

Resultado de un **suceso** (3.25) que afecta a los **objetivos** (3.56).

[Guía ISO 73:2009]

NOTA 1: Un suceso puede conducir a una serie de consecuencias.
NOTA 2: Una consecuencia puede ser cierta o incierta y normalmente es negativa en el contexto de la seguridad de la información.
NOTA 3: Las consecuencias se pueden expresar de forma cualitativa o cuantitativa.
NOTA 4: Las consecuencias iniciales pueden convertirse en reacciones en cadena.

3.15 Mejora Continua

Actividad recurrente para mejorar el **desempeño** (3.59).

3.16 Control

Medida que modifica un **riesgo** (3.68).

[ISO Guía 73:2090]

NOTA 1: Los controles incluyen cualquier proceso, política, dispositivo, práctica, u otras acciones que modifiquen un riesgo.

NOTA 2: Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

3.17 Objetivo de Control

Declaración que describe lo que se quiere lograr como resultado de la implementación de **controles** (3.16).

3.18 Corrección

Acción para eliminar una **no conformidad** (3.53) detectada.

3.19 Acción Correctiva

Acción para eliminar la causa de una **no conformidad** (3.53) y prevenir que vuelva a ocurrir.

3.20 Datos

Conjunto de valores asociados a **medidas básicas** (3.10), **medida derivadas** (3.22) y/o **indicadores** (3.30).

[ISO/IEC 15939:2007]

NOTA: Esta definición solo se aplica en el contexto de la Norma ISO/IEC 27004:2009.

3.21 Criterios de Decisión

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

[ISO/IEC 15939:2007]

3.22 Medida Derivada

Medida (3.47) que se define en función de dos o más valores de **medidas básicas** (3.10).

[ISO/IEC 15939:2007]

3.23 Información Documentada

Información que una **organización** (3.57) tiene que controlar y mantener, y el medio en el que está contenida.

NOTA 1: La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2: La información documentada puede hacer referencia a:

- El **sistema de gestión** (3.46), incluidos los **procesos** (3.61) relacionados.
- La información creada para que la organización opere (documentación).
- La evidencia de los resultados alcanzados (registros).

3.24 Eficacia

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

3.25 Evento

Ocurrencia o cambio de un conjunto particular de circunstancias.

[Equivalente a “suceso” en Guía ISO 73:2009]

NOTA 1: Un evento puede ser único o repetirse, y se puede deber a varias causas.

NOTA 2: Un evento puede consistir en algo que no se llega a producir.

NOTA 3: Algunas veces, un evento se puede calificar como un “incidente” o un “accidente”.

3.26 Dirección Ejecutiva

Persona o grupo de persona en la(s) que los **órganos de gobierno** (3.29) han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la **organización** (3.57).

NOTA: La dirección ejecutiva a veces se llama alta dirección y puede incluir directores generales, directores financieros, directores de la información y otros roles similares.

3.27 Contexto Externo

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

[Guía ISO 73:2009]

NOTA: El entorno externo puede incluir:

- El entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local.
- Los factores y las tendencias que tengan impacto sobre los **objetivos** (3.56) de la **organización** (3.57).
- Las relaciones con las **partes interesadas** externas (3.82), sus percepciones y sus valores.

3.28 Gobernanza de la Seguridad de la Información

Conjunto de principios y **procesos** (3.61) mediante los cuales una **organización** (3.57) dirige y supervisa las actividades relacionadas con la seguridad de la información.

3.29 Órgano de Gobierno

Conjunto de personas que responden y rinden cuentas del **desempeño** (3.59) de la **organización** (3.57).

NOTA: En algunas jurisdicciones, el órgano de gobierno puede ser el consejo de administración.

3.30 Indicador

Medida (3.47) que proporciona una estimación o una evaluación de determinados **atributos** (3.4) usando un **modelo analítico** (3.2) para satisfacer unas determinadas **necesidades de información** (3.31).

3.31 Necesidades de Información

Conocimiento necesario para gestionar los objetivos, las metas, el riesgo y los problemas.

[ISO/IEC 15939:2007]

3.32 Recursos (*instalaciones*) de Tratamiento de Información

Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

3.33 Seguridad de la Información

Preservación de la **confidencialidad** (3.12), la **integridad** (3.40) y la **disponibilidad** (3.9) de la información.

NOTA: Pudiendo, además, abarcar otras propiedades, como la **autenticidad** (3.8), la responsabilidad, el **no repudio** (3.54) y la **fiabilidad** (3.62).

3.34 Continuidad de la Seguridad de la Información

Procesos (3.61) y procedimientos para asegurar la continuidad de las actividades relacionadas con la **seguridad de la información** (3.33).

3.35 Evento o Suceso de Seguridad de la Información

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

3.36 Incidente de Seguridad de la Información

Evento singular o serie de **eventos de la seguridad de la información** (3.35), inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la **seguridad de la información** (3.33).

3.37 Gestión de Incidentes de Seguridad de la Información

Procesos (3.61) para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de **incidentes de la seguridad de la información** (3.36).

3.38 Colectivo que Comparte Información

Grupo de organizaciones que acuerdan compartir información.

NOTA: Una organización puede ser un individuo.

3.39 Sistema de Información

Aplicaciones, servicios, activos de tecnologías de la información y otro componentes para manejar información.

3.40 Integridad

Propiedad de exactitud y completitud.

3.41 Parte Interesada

Persona u **organización** (3.57) que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

3.42 Contexto Interno

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

[Guía ISO 73:2009]

NOTA: El contexto interno puede incluir:

- El gobierno, la estructura de la organización, las funciones y la obligación de rendir cuentas.
- Las políticas, los objetivos y las estrategias que se establecen para conseguirlo.
- Las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).
- Los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales).
- Las relaciones, percepciones y los valores de las partes interesadas internas.
- La cultura de la organización.
- Las normas, las directrices y los modelos adoptados por la organización.
- La forma y amplitud de las relaciones contractuales.

3.43 Proyecto del SGSI

Actividades estructurales llevadas a cabo por una **organización** (3.57) para implementar un SGSI.

3.44 Nivel de Riesgo

Magnitud de un **riesgo** (3.68) o combinación de riesgos, expresados en términos de la combinación de las **consecuencias** (3.14) y de su **probabilidad** (3.45).

[Guía ISO 73:2009]

3.45 Probabilidad *(likehood)*

Posibilidad de que algún hecho se produzca.

[Guía ISO 73:2009]

3.46 Sistema de Gestión

Conjunto de elementos de una **organización** (3.57) interrelacionados o que interactúan para establecer **políticas** (3.60), **objetivos** (3.56) y **procesos** (3.61) para lograr estos objetivos.

NOTA 1: Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 2: Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, etc.

NOTA 3: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

3.47 Medida

Variable a la que se le asigna un valor como resultado de una **medición** (3.48).

[ISO/IEC 15939:2007]

NOTA: El termino “medidas” se utiliza para hacer referencia conjuntamente a medidas de base, de las derivadas, e indicadores.

3.48 Medición

Proceso (3.61) para determinar un valor.

NOTA: En el contexto de **seguridad de la información** (3.33), el proceso para determinar un valor requiere información sobre la **eficacia** (3.24) de un **sistema de gestión** (3.46) de seguridad de la información y sus correspondientes **controles** (3.16) utilizando un **método de medición** (3.50), una **función de medición** (3.49), un **modelo analítico** (3.2), y unos **criterios de decisión** (3.21).

3.49 Función de Medición

Algoritmo o cálculo realizado para combinar dos o más **medidas básicas** (3.10).

[ISO/IEC 15939:2007]

3.50 Método de Medición

Secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un **atributo** (3.4) con respecto a una **escala** (3.80) especificada.

[ISO/IEC 15939:2007]

NOTA: El tipo de método de medición depende de la naturaleza de las operaciones utilizadas para cuantificar un atributo. Se pueden distinguir dos tipos:

- Subjetivo: La cuantificación se basa en el juicio humano.
- Objetivo: La cuantificación se basa en reglas numéricas.

3.51 Resultados de las Mediciones

Uno o más **indicadores** (3.30) y sus correspondientes interpretaciones que abordan una necesidad de **información** (3.31).

3.52 Supervisión, Seguimiento o Monitorización (monitoring)

Determinación del estado de un sistema, un **proceso** (3.61) o una actividad.

NOTA: Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

3.53 No Conformidad

Incumplimiento de un **requisito** (3.63).

3.54 No Repudio

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.

3.55 Objeto

Elemento caracterizado por medio de la **medición** (3.48) de sus **atributos** (3.4).

3.56 Objetivo

Resultado a lograr

NOTA 1: Un objetivo puede ser estratégico, táctico u operativo.

NOTA 2: Los objetivos pueden referirse a diferentes disciplinas (como financieras, de seguridad y salud y ambientales) y se pueden aplicar en diferentes niveles (como estratégicos, para toda la organización, para proyectos, productos y **procesos** (3.61)).

NOTA 3: Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de seguridad de la información, o mediante el uso de términos con un significado similar (por ejemplo, finalidad o meta).

NOTA 4: En el contexto de sistemas de gestión de la seguridad de la información, la organización establece los objetivos de la seguridad de la información, en concordancia con la política de seguridad de la información, para lograr resultados específicos.

3.57 Organización

Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus **objetivos** (3.56).

NOTA: El concepto de organización incluye, pero no se limita a, empresarios unipersonales, empresas, corporaciones, firmas, autoridades, asociaciones, etc., en si mismas, parcialmente o grupo de ellas, sean públicas o privadas.

3.58 Contratar Externamente (verbo)

Establecer un acuerdo mediante el cual una **organización** (3.57) externa realiza parte de una función o **proceso** (3.61) de una organización.

NOTA 1: Una organización externa está fuera del alcance del **sistema de gestión** (3.46), aunque la función o proceso contratado externamente forme parte del alcance.

3.59 Desempeño

Resultado medible.

NOTA 1: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

NOTA 2: El desempeño se puede relacionar con la gestión de actividades, **procesos** (3.61), productos (incluidos servicios), sistemas u **organizaciones** (3.57).

3.60 Política

Intenciones y dirección de una **organización** (3.57), como las expresa formalmente su **alta dirección** (3.84).

3.61 Proceso

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

3.62 Fiabilidad

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

3.63 Requisito

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

NOTA 1: “Generalmente implícita” significa que es una costumbre o práctica común en la organización y en las partes interesadas, que la necesidad o expectativa que se considera está implícita.

NOTA 2: Un requisito especificado es el que está declarado, por ejemplo, en información documentada.

3.64 Riesgo Residual

Riesgo (3.68) remanente después del **tratamiento del riesgo** (3.79).

NOTA 1: El riesgo residual puede contener riesgos no identificados.

NOTA 2: El riesgo residual también se puede conocer como “riesgo retenido”.

3.65 Revisión

Actividad que se realiza para determinar la idoneidad, la adecuación y la **eficacia** (3.24) del tema estudiado para conseguir los objetivos establecidos.

[Guía ISO 73:2009]

3.66 Objeto en Revisión

Elemento específico que está siendo revisado.

3.67 Objetivo de la Revisión

Declaración que describe lo que se quiere lograr como resultado de una revisión.

3.68 Riesgo

Efecto de la incertidumbre sobre la consecución de los objetivos.

[Guía ISO 73:2009]

NOTA 1: Un efecto es una desviación, positiva y/o negativa, respecto a lo provisto.

NOTA 2: La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un **suceso** (3.25), de sus **consecuencias** (3.14) o de su **probabilidad** (3.45).

3.68 Riesgo

NOTA 3: Con frecuencia, el riesgo se caracteriza por referencia a **sucesos** (3.25) potenciales y a sus **consecuencias** (3.14) o una combinación de ambos.

NOTA 4: Con frecuencia, el riesgo se expresa en términos de combinación de las **consecuencias** (3.14) de un suceso (incluyendo los cambios en las circunstancias) y de su **probabilidad** (3.45).

NOTA 5: En el contexto de sistema de gestión de la seguridad de la información, los riesgos de seguridad de la información se pueden expresar como el efecto de la incertidumbre sobre los objetivos de seguridad de la información.

NOTA 6: El riesgo de seguridad de la información se relaciona con la posibilidad de que las **amenazas** (3.83) exploten **vulnerabilidades** (3.89) de un activo o grupo de activos de información y causen daño a una organización.

3.69 Aceptación del Riesgo

Decisión informada en favor de tomar un **riesgo** (3.68) particular.

[Guía ISO 73:2009]

NOTA 1: La aceptación del riesgo puede tener lugar sin que exista **tratamiento del riesgo** (3.79) o durante el proceso de tratamiento del riesgo.

NOTA 2: Los riesgos aceptados son objeto de **seguimiento** (3.52) y de **revisión** (3.65).

3.70 Análisis del Riesgo

Proceso que permite comprender la naturaleza del **riesgo** (3.68) y determinar el **nivel de riesgo** (3.44).

[Guía ISO 73:2009]

NOTA 1: El análisis del riesgo proporciona las bases para la **evaluación del riesgo** (3.74) y para tomar las decisiones relativas al **tratamiento del riesgo** (3.79).

NOTA 2: El análisis del riesgo incluye la estimación del riesgo.

3.71 Apreciación del Riesgo

Proceso (3.61) global que comprende la **identificación del riesgo** (3.75), el **análisis del riesgo** (3.70) y la **evaluación del riesgo** (3.74).

[Guía ISO 73:2009]

3.72 Comunicación y Consulta del Riesgo

Procesos iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las **partes interesadas** (3.82), en relación con la gestión del **riesgo** (3.68).

[Guía ISO 73:2009]

NOTA 1: La información puede corresponder a la existencia, la naturaleza, la forma, la probabilidad, la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del riesgo.

NOTA 2: La consulta constituye un proceso de comunicación informada de doble sentido entre una organización y sus partes interesadas, sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

- Un proceso que impacta sobre una decisión a través de la influencia más que por la autoridad.
- Una contribución para una toma de decisión y no una toma de decisión conjunta.

3.73 Criterios de Riesgo

Términos de referencia respecto a los que se evalúa la importancia de un **riesgo** (3.68).

[Guía ISO 73:2009]

NOTA 1: Los criterios de riesgo se basan en los objetivos de la organización y en el contexto externo e interno.

NOTA 2: Los criterios de riesgo se puede obtener de normas, leyes, políticas y otros requisitos.

3.74 Evaluación del Riesgo

Proceso (3.61) de comparación de los resultados del **análisis de riesgo** (3.70) con los **criterios de riesgo** (3.73) para determinar si el **riesgo** (3.68) y/o su magnitud son aceptables o tolerables.

[Guía ISO 73:2009]

NOTA: La evaluación del riesgo ayuda a la toma de decisiones sobre el **tratamiento del riesgo** (3.79).

3.75 Identificación del Riesgo

Proceso que comprende la búsqueda, el reconocimiento y la descripción de los **riesgos** (3.68).

[Guía ISO 73:2009]

NOTA 1: La identificación del riesgo implica la identificación de las fuentes de riesgos, los sucesos, sus causas y sus consecuencias potenciales.

NOTA 2: La identificación del riesgo puede implicar datos históricos, análisis teóricos, opiniones informadas y de expertos, así como necesidades del las partes interesadas.

3.76 Gestión del Riesgo

Actividades coordinadas para dirigir y controlar una **organización** (3.57) en lo relativo al **riesgo** (3.68).

[Guía ISO 73:2009]

3.77 Proceso de Gestión del Riesgo

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del **riesgo** (3.68).

[Guía ISO 73:2009]

NOTA: La Norma ISO/IEC 27005 utiliza el término “proceso” para describir la gestión integral del riesgo. Los elementos dentro del proceso de gestión del riesgo se denominan “actividades”.

3.78 Dueño del Riesgo

Persona o entidad que tiene la responsabilidad y autoridad para gestionar un **riesgo** (3.68).

[Guía ISO 73:2009]

3.79 Tratamiento del Riesgo

Proceso (3.61) destinado a modificar el **riesgo** (3.68).

[Guía ISO 73:2009]

NOTA 1: El tratamiento del riesgo puede implicar:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que motiva el riesgo.
- Aceptar o aumentar el riesgo con el objeto de buscar una oportunidad.
- Eliminar la fuente de riesgo.
- Cambiar la probabilidad.
- Cambiar las consecuencias.
- Compartir el riesgo con otra u otras partes (incluyendo los contratos y la financiación del riesgo).
- Mantener el riesgo en base a una decisión informada.

3.79 Tratamiento del Riesgo

NOTA 2: Los tratamientos del riesgo que conducen a consecuencias negativas, en ocasiones se citan como “mitigación del riesgo”, “eliminación del riesgo”, “prevención del riesgo” y “reducción del riesgo”.

NOTA 3: El tratamiento del riesgo puede originar nuevos riesgos o modificar los riesgos existentes.

3.80 Escala

Conjunto ordenado de valores, continuo o discreto, o un conjunto de categorías a las que se asigna el **atributo** (3.4).

[ISO/IEC 15939:2007]

NOTA: El tipo de escala depende de la naturaleza de la relación entre los valores de la escala. Comúnmente se identifican cuatro tipos de escala:

1. Nominal: Los valores de medición son categorías.
2. Ordinal: Los valores de medición son categorías ordenadas.
3. Intervalo: Los valores de las mediciones se ajustan a rangos de valores cuantitativos del atributo.
4. Proporción: Los valores de las mediciones son relativos y proporcionales al valor de otro atributo; correspondiendo el valor cero al valor cero del atributo.

Estos son solo ejemplos de tipos de escala.

3.81 Norma de Implementación de la Seguridad

Documento que especifica las formas autorizadas para satisfacer las necesidades de seguridad.

3.82 Parte Interesada

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

[ISO/IEC 73:2009]

3.83 Amenaza

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

3.84 Alta Dirección

Persona o grupo de personas que dirigen y controlan una **organización** (3.57) al más alto nivel.

NOTA 1: La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

NOTA 2: Si el alcance del **sistema de gestión** (3.46) comprende solo una parte de una organización, entonces “alta dirección” se refiere a quienes dirigen y controlan esa parte de la organización.

3.85 Entidad de Confianza para la Comunicación de la Información

Organización independiente que sustenta el intercambio de información dentro de un colectivo que comparte información.

3.86 Unidad de Medida

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

[ISO/IEC 15939:2007]

3.87 Validación

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

[ISO/IEC 9000:2005]

3.88 Verificación

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

[ISO/IEC 9000:2005]

NOTA: También podría llamarse prueba de conformidad.

3.89 Vulnerabilidad

Debilidad de un activo o de un **control** (3.16) que puede ser explotada por una o más **amenazas** (3.83).

3.90 Información

Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

3.91 Activo

Algo de valor para la organización , ya sea tangible o intangible, que es necesario proteger, incluyendo personal, hardware, software, servicios, infraestructura, documentos, datos entre otros.

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

#I27001F #certiprof

certiprof®

¡Síguenos, ponte en contacto!

www.certiprof.com