https://view.genial.ly/65de6c9b6f2f120014a774cb/presentation-presentacion-justicia

NORMA ISO-27001  
CAPÍTULO 4

**\_\_\_**

– Jose Luis Tamara, Camilo Hernandez, Esteban Isaza, Josué David Gonzalez. —

# INTRODUCCIÓN

El capítulo 4 de la ISO/IEC 27001 se centra en el contexto de la organización, y su título es "Contexto de la organización"

## 4. Contexto de la organización

Este capítulo se centra en comprender el contexto de la organización y su impacto en la gestión de la seguridad de la información (SGSI). se dividen en tres subcapítulos.

## 4.1 Comprensión de la organización y contexto.

**4.1.1 Comprensión de la organización:**

* La organización debe comprender su propósito y dirección estratégica, incluyendo su misión, visión, valores y objetivos.
* Debe identificar las partes interesadas relevantes y sus necesidades y expectativas relacionadas con la SGSI.

**4.1.2 Comprensión del contexto externo:**

* La organización debe identificar los factores externos que pueden afectar a su SGSI, como tendencias del mercado, cambios tecnológicos, requisitos legales y reglamentarios, y riesgos y oportunidades sociales, culturales, económicas y ambientales.

**4.1.3 Comprensión del contexto interno:**

* La organización debe identificar los factores internos que pueden afectar a su SGSI, como su cultura, estructura, valores, procesos y recursos.

**4.2 Comprensión de las necesidades y expectativas de las partes interesadas:**

* La organización debe identificar las necesidades y expectativas de las partes interesadas relevantes, como clientes, empleados, proveedores, socios y reguladores.
* Debe considerar estas necesidades y expectativas al establecer, implementar y mantener la SGSI.

**4.3 Determinación del alcance del sistema de gestión de la seguridad de la información:**

* La organización debe determinar el alcance de su SGSI, incluyendo los procesos, funciones, activos y personas que estarán dentro del alcance.
* El alcance debe ser documentado y estar disponible para las partes interesadas relevantes.

**4.4 Sistema de gestión de la seguridad de la información:**

* La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI que cumpla con los requisitos de la norma ISO 27001.
* El SGSI debe estar documentado y ser apropiado para la naturaleza, escala y complejidad de las actividades de la organización.

**4.5 Enfoque basado en procesos:**

* La organización debe aplicar un enfoque basado en procesos al implementar y gestionar su SGSI.
* Esto implica identificar, comprender y gestionar los procesos interrelacionados que conforman la SGSI.

**4.6 Liderazgo:**

* La alta dirección debe demostrar su liderazgo y compromiso con la SGSI.
* Esto incluye proporcionar recursos, asignar responsabilidades y comunicar la importancia de la SGSI a toda la organización.

**4.7 Política de seguridad de la información:**

* La alta dirección debe establecer y mantener una política de seguridad de la información que sea apropiada para la organización.
* La política debe definir el compromiso de la organización con la seguridad de la información y proporcionar un marco para la gestión de la SGSI.

**4.8 Roles, responsabilidades y autoridades:**

* La organización debe definir y documentar los roles, responsabilidades y autoridades para la gestión de la SGSI.
* Esto debe incluir la asignación de responsabilidades para la implementación, mantenimiento y mejora de la SGSI.

**4.9 Competencia:**

* La organización debe asegurarse de que las personas que trabajan bajo su control tengan la competencia necesaria para realizar sus tareas de forma que se asegure la conformidad con la SGSI.
* Esto incluye la provisión de formación y concienciación sobre la seguridad de la información.

**4.10 Concienciación:**

* La organización debe concienciar a todos los miembros del personal sobre la importancia de la SGSI y sus responsabilidades individuales.
* Esto debe incluir la formación sobre las políticas y procedimientos de seguridad de la información.

**4.11 Comunicación:**

* La organización debe establecer e implementar un proceso de comunicación eficaz para la SGSI.
* Esto debe incluir la comunicación interna y externa sobre la seguridad de la información.

**4.12 Documentación:**

* La organización debe establecer y mantener un sistema de documentación para la SGSI.
* La documentación debe incluir la política de seguridad de la información, los objetivos de la SGSI, los planes de gestión de riesgos y los registros de las actividades de la SGSI.

**4.13 Control de la documentación:**

* La organización debe controlar la documentación de la SGSI para asegurar su integridad, confidencialidad y disponibilidad.

**4.14 Operación:**

* La organización debe planificar, implementar y controlar las operaciones de la SGSI para cumplir con los requisitos