

# NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001

## Concepto

La NTC-ISO/IEC 27001 en Colombia adapta la norma global ISO/IEC 27001 para establecer un Sistema de Gestión de Seguridad de la Información. Enfocado en identificar activos valiosos, evaluar riesgos, aplicar protecciones y mantener mejora constante, fortalece la seguridad de datos y aumenta la confianza en la organización.



## Aplicación

La aplicación de la norma NTC-ISO/IEC 27001 implica seguir un proceso estructurado para gestionar la seguridad de la información en una organización:

- Identificación de activos de información
- Evaluación de riesgos.
- Implementación de medidas de seguridad
- Establecimiento de sistema de gestión.
- Monitoreo y mejora continua
- Cumplimiento y certificación.
- Educación y concienciación..



## ¿Qué es SGSI?

Un SGSI es un sistema organizado que gestiona la seguridad de la información, protegiendo su confidencialidad, integridad y disponibilidad. Se basa en estándares como ISO/IEC 27001 y abarca desde la identificación de riesgos hasta la implementación de controles y la mejora continua. Su objetivo es minimizar amenazas y riesgos cibernéticos para mantener segura la información sensible de una organización.

## SGSI en las empresas

En las empresas, un SGSI (Sistema de Gestión de Seguridad de la Información) es un enfoque estructurado para proteger datos importantes. Utiliza estándares como ISO/IEC 27001, abordando desde la identificación de riesgos hasta la implementación de medidas y mejoras constantes. Busca minimizar amenazas cibernéticas y asegurar la confidencialidad, integridad y disponibilidad de la información valiosa de la empresa.

## Requisitos de Documentación

La norma ISO/IEC 27001 establece varios requisitos de documentación que deben ser cumplidos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo.

1. **Política de Seguridad de la Información:** Una declaración formal de los objetivos y compromisos de la organización en materia de seguridad de la información.
2. **Alcance del SGSI:** Una descripción clara de los límites y aplicabilidad del SGSI en la organización.
3. **Procedimientos documentados:** Documentos que describen los procedimientos específicos que se deben seguir para llevar a cabo actividades de seguridad, como la gestión de incidentes, el control de acceso, la clasificación de la información, etc.

# Responsabilidad de la Direccion



## Compromiso y apoyo

Los líderes deben demostrar un compromiso activo hacia la seguridad de la información y brindar los recursos necesarios para implementar y mantener el SGSI de manera efectiva.

Definir la política de seguridad: La alta dirección debe establecer una Política de Seguridad de la Información que refleje los objetivos de seguridad y los compromisos de la organización.

## Establecer el alcance

Determinar el alcance del SGSI, definiendo qué activos y procesos estarán cubiertos por el sistema.

## Liderazgo

Dirigir y fomentar la cultura de seguridad en toda la organización, comunicando la importancia de la seguridad de la información y alentando la participación de todos.

## Designar roles y responsabilidades

Asignar responsabilidades claras a nivel de la dirección y en toda la organización para la gestión de la seguridad de la información.

## Revisión y mejora

Participar en la revisión periódica del SGSI para asegurarse de que esté funcionando adecuadamente y tomar decisiones para la mejora continua.

## Participación activa

Los líderes deben involucrarse activamente en la toma de decisiones sobre cuestiones de seguridad de la información, incluyendo la aprobación de inversiones en medidas de seguridad y la gestión de riesgos.

## Comunicación

Comunicar de manera efectiva la importancia de la seguridad de la información a todos los niveles de la organización, así como a socios externos y partes interesadas.