



ISO/IE 27001

Seguridad de la Información y Gobernanza Digital

Lisseth Orduz
Luis Cardenas

¿Qué es?

- Es una Norma Técnica Colombiana (NTC) que es idéntica (IDT) por traducción a la norma internacional ISO/IEC 27001:2022.
- En pocas palabras: Es un Sistema de Gestión de Seguridad de la Información (SGSI) que te da los requisitos para proteger los datos de una organización.
- Objetivo Clave: Preservar la confidencialidad, la integridad y la disponibilidad de la información



Generalidades y Base del SGSI

(Introducción y Cláusulas 1 a 3)

- Es una Decisión Estratégica: Implementar este sistema es una elección clave para la empresa. No es solo un tema técnico.
- ¿A quién aplica? Es genérica y aplica a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.
- Su Estructura: Utiliza la "Estructura de Alto Nivel" (Anexo SL), lo que la hace compatible y fácil de integrar con otras normas de gestión (como la ISO 9001, ISO 14001, etc.).
- El SGSI busca: Dar confianza a las partes interesadas de que los riesgos de seguridad se están gestionando adecuadamente.





Cláusula 4: Contexto de la Organización

- 4.1 Comprensión del Contexto: Tienes que determinar qué cuestiones externas e internas (políticas, económicas, culturales, tecnológicas, etc.) son relevantes para tu propósito y afectan a tu SGSI.
- 4.2 Partes Interesadas: Identifica a quién le importa tu seguridad (clientes, reguladores, empleados, proveedores) y cuáles son sus requisitos (incluyendo legales y contractuales).
- 4.3 Determinación del Alcance: Define los límites de tu SGSI. ¿Qué áreas, procesos o ubicaciones cubre? Esto debe quedar como información documentada.
- 4.4 Sistema de Gestión: La obligación de establecer, implementar, mantener y mejorar continuamente el SGS



Cláusula 5: Liderazgo



- 5.1 Liderazgo y Compromiso: La alta dirección debe asegurar que la política y los objetivos de seguridad son compatibles con la estrategia general de la organización, que hay recursos y que se promueve la mejora continua.
- 5.2 Política de Seguridad: Debe ser un documento formal que incluya el compromiso de satisfacer requisitos y de la mejora continua del sistema. Debe ser comunicada y estar documentada.
- 5.3 Roles, Responsabilidades y Autoridades: Define y comunica quién es responsable de qué dentro del SGSI.

Cláusula 6: Planificación

6.1 Acciones para abordar riesgos y oportunidades:

- Determinar los riesgos y oportunidades para asegurar que el SGSI pueda lograr sus resultados previstos y para prevenir o reducir efectos no deseados.
- Se debe definir un proceso para la Evaluación de Riesgos (identificar riesgos, analizar consecuencias y probabilidades, determinar niveles).
- También se define el Tratamiento de Riesgos (seleccionar controles, producir una Declaración de Aplicabilidad o SoA, y obtener la aceptación de los dueños de los riesgos).
- 6.2 Objetivos de Seguridad: Los objetivos deben ser coherentes con la política, medibles (si es posible), monitoreados y comunicados. Se debe planificar:
 - qué se hará, qué recursos se necesitarán, quién será responsable y cómo se evaluarán los resultados.
- 6.3 Planificación de los Cambios: Cualquier cambio al SGSI debe hacerse de forma planificada.



Cláusula 7: Apoyo

- 7.1 Recursos: Determinar y proporcionar los recursos necesarios (personal, tecnología, dinero).
- 7.2 Competencia: Asegurarse de que las personas que trabajan en el SGSI son competentes (con educación, formación o experiencia adecuadas).
- 7.3 Toma de Conciencia: El personal debe ser consciente de la política de seguridad, de su contribución y de las implicaciones de no cumplir con los requisitos.
- 7.4 Comunicación: Determinar las necesidades de comunicación (qué, cuándo, a quién y cómo).
 - 7.5 Información Documentada:
El SGSI debe incluir la información requerida por la norma y la que la organización determine necesaria para la
 - eficacia del sistema.
 - Se deben establecer controles (distribución, protección, control de versiones, retención).



Cláusula 8: Operación

- 8.1 Planificación y Control de la Operación: Planificar, implementar y controlar los procesos para cumplir con el numeral 6, incluyendo el establecimiento de criterios para los procesos y la implementación de controles.
- 8.2 Evaluación de Riesgos: Realizar las evaluaciones a intervalos planificados o cuando ocurran cambios significativos.
- 8.3 Tratamiento de Riesgos: Implementar el plan de tratamiento de riesgos.



Cláusula 9: Evaluación del Desempeño



9.1 Seguimiento, Medición, Análisis y Evaluación: Determinar qué, cómo y cuándo hacer seguimiento y medir, y evaluar el desempeño y la eficacia del SGSI.

9.2 Auditoría Interna: Realizar auditorías internas planificadas para obtener información sobre si el SGSI es conforme con los requisitos propios y los de la norma.

9.3 Revisión por la Dirección: La alta dirección debe revisar el sistema a intervalos planificados para asegurar su conveniencia, adecuación y eficacia continuas. Las salidas de esta revisión deben incluir decisiones relacionadas con la mejora continua.

Cláusula 10: Mejora

El ciclo de mejora continua.

- 10.1 Mejora Continua: La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.
- 10.2 No Conformidad y Acción Correctiva: Cuando ocurra una no conformidad (algo que no cumple con un requisito): reaccionar ante ella y tomar acciones para corregirla.
- Evaluar la necesidad de acciones para eliminar la causa raíz de la no conformidad y evitar que vuelva a ocurrir.

Anexo A (Normativo):

Los Controles

Este anexo es normativo, lo que significa que es obligatorio revisarlo.

Contiene una

- referencia de los controles de seguridad de la información que la organización puede seleccionar para el tratamiento de riesgos.
- Enfoque de la norma: Los controles se dividen en cuatro secciones (aunque la Tabla A.1 solo muestra tres categorías principales de controles):
 1. Controles Organizacionales (Ej: Políticas de seguridad, Roles, Procesos Disciplinarios).
 2. Controles de Personas (Ej: Competencia, Conciencia, Acuerdos de Confidencialidad).
 3. Controles Físicos (Ej: Perímetros de Seguridad, Entradas, Monitoreo de Seguridad Física).
 4. Controles Tecnológicos (Ej: Gestión de Acceso, Criptografía, Gestión de Vulnerabilidades).



MUCHAS GRACIAS

