UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 4:

Implementación y Gestión en el Estándar ISO 27001

Sesión 1:

Introducción a ISO/IEC 27001 y el Sistema de Gestión de Seguridad de la Información (SGSI)

OBJETIVO DE LA SESIÓN:

Comprender los fundamentos de ISO/IEC 27001:2022, su estructura, objetivos y beneficios, así como los conceptos clave del Sistema de Gestión de Seguridad de la Información (SGSI).

¿Qué es ISO/IEC 27001?

ISO/IEC 27001:2022 es una **norma internacional** que establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

Propósito:
Ayudar a las organizaciones a proteger su información mediante la gestión de riesgos y la implementación de controles adecuados.

¿Por qué es importante?

Reconocimiento internacional
Mejora la reputación de la organización.

Cumplimiento de clientes y regulaciones
Muchas empresas exigen esta certificación a sus proveedores.

Gestión de riesgos efectiva
Permite identificar, tratar y monitorear riesgos de forma estructurada.

Confianza de las partes interesadas
Asegura clientes, empleados y socios que su información está protegida.

Estructura general de ISO/IEC 27001:2022

Cláusulas principales (requisitos)

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 continua

Anexo A

Lista de 93 controles divididos en 4 categorías:

- Controles organizacionales
- Controles de personas
- Controles físicos
- Controles tecnológicos

Principales conceptos

Concepto	Explicación básica
Activo de información	Todo aquello que tiene valor para la organización (datos, software, personas, infraestructura).
Riesgo	Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto.
Amenaza	Evento potencial que puede dañar un activo (ej. malware, fallo humano, desastres naturales).
Vulnerabilidad	Debilidad que puede ser explotada por una amenaza.
Control	Medida para reducir un riesgo. Ej. contraseña segura, backup.

Identificación de activos

Todo recurso que tiene valor para la organización.

Hardware: servidores, laptops, móviles.

Software: sistemas, aplicaciones, bases de datos.

Personas: empleados, contratistas, proveedores.

Datos: registros de clientes, historias clínicas.

Instalaciones: oficinas, centros de datos.

Importancia: sin inventario claro, no se pueden proteger.

Clasificación de los activos de información

Críticos
imprescindibles para la operación, su pérdida detiene la organización
Ejemplo: Servidor de base de datos de pacientes en un hospital.

Sensibles
contienen información que, si se filtra, afecta a clientes o procesos.
Ejemplo: Nómina de empleados.

Confidenciales
acceso restringido, solo personal autorizado.
Ejemplo: Contratos con proveedores estratégicos.

Públicos
información de libre acceso, no compromete la seguridad.
Ejemplo: Página web institucional.

Banco Comercial

Activo	Tipo	Clasificación
Base de datos de clientes (cuentas, transacciones)	Datos	Crítico / Sensible
Servidores de banca en línea	Hardware	Crítico
Aplicación móvil de clientes	Software	Sensible / Confidencial
Cajeros automáticos (ATM)	Hardware	Sensible
Personal de atención al cliente	Personas	Confidencial
Portal web público (informativo)	Software	Público

Ejemplo: Hospital Universitario

Activo	Tipo	Clasificación
Historias clínicas electrónicas	Datos	Crítico / Sensible
Servidores de aplicaciones	Hardware	Crítico
Dispositivos médicos conectados (monitores, bombas de infusión)	Hardware	Sensible
Personal médico autorizado	Personas	Confidencial
Sitio web público	Software	Público

¿Cómo evaluamos los riesgos?

Probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto.

Riesgo = Amenaza × Vulnerabilidad × Impacto

Tipos de impacto

Reputacional: pérdida de confianza del cliente
Económico: multas, sanciones, pérdidas
Legal: incumplimiento normativo
Operativo: caída de sistemas críticos.

Fuga de datos por correo mal enviado

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Impacto	Acción de mitigación
Fuga de datos	Falta de capacitación del personal	Reputacional (pérdida de confianza), Legal (sanciones por Habeas Data)	Medio	Alto	Implementar capacitación, activar revisión de correos sensibles, cifrado de adjuntos

En ISO 27001 y metodologías de gestión de riesgos, el cálculo de riesgo suele hacerse con una fórmula simplificada:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Donde:

- Probabilidad y Impacto se miden en escalas (Bajo = 1, Medio = 2, Alto = 3).
- Multiplicando ambos valores, se obtiene un nivel de riesgo numérico, que luego se traduce en cualitativo (Bajo, Medio, Alto).

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Robo de dispositivo (laptop de un empleado)

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Impacto	Acción de mitigación
Robo físico	Dispositivo sin cifrado	Económico (pérdida de información), Reputacional (exposición de datos), Operativo (interrupción de trabajo)	2 (Medio)	3 (Alto)	Cifrado de disco, uso de contraseñas fuertes, políticas de bloqueo remoto

Riesgo = Probabilidad × Impacto

Acceso no autorizado a base de datos

Amenaza	Vulnerabilidad	Impacto	Probabilidad	Impacto	Acción de mitigación
Acceso no autorizado	Contraseñas débiles	Legal (sanciones regulatorias), Económico (multas), Operativo (interrupción de servicio)	3 (Alto)	3 (Alto)	Implementar MFA, rotación de contraseñas, monitoreo de accesos

Riesgo = Probabilidad × Impacto

¿Qué es un SGSI?

Un **Sistema de Gestión de Seguridad de la Información (SGSI)** es un conjunto de políticas, procesos, procedimientos y controles interrelacionados que permiten gestionar la seguridad de la información de forma sistemática y continua.

Ejemplo práctico

Una universidad implementa su SGSI definiendo:

- Su política de seguridad.
- Procedimientos para el uso seguro de plataformas virtuales.
- Controles como autenticación de doble factor para acceso a notas y matrículas.
- Evaluación anual de sus riesgos y auditoría interna.

Opciones de tratamiento del riesgo

Mitigar → reducir el riesgo con controles (ej. instalar firewall, actualizar parches).

Aceptar → cuando el costo de mitigación es mayor al impacto (ej. riesgo bajo documentado).

Transferir → pasar el riesgo a un tercero (ej. seguro cibernético, outsourcing).

Evitar → eliminar la actividad de riesgo (ej. no usar USB en equipos críticos).

Ejemplos de acciones

Riesgo	Acción de tratamiento	Ejemplo
Ataque de ransomware	Mitigar	Instalar EDR y copias de seguridad offline
Pérdida económica por brecha	Transferir	Contratar seguro cibernético
Acceso a datos en USB	Evitar	Política de bloqueo de puertos USB
Caída de app secundaria	Aceptar	Documentar y asumir impacto bajo

Gestión de riesgos efectiva

- Identificar activos críticos y vulnerabilidades.
- Evaluar la probabilidad e impacto de las amenazas.
- Clasificar riesgos (bajo, medio, alto).
- Definir planes de tratamiento (mitigar, transferir, aceptar, evitar).
- Monitorear y mejorar continuamente (ciclo PHVA).

Ejercicio 1: Reflexión inicial grupal

¿Qué activo consideras crítica en tu contexto personal, académico o laboral, y qué pasaría si se ve comprometida?

Ejercicio 2: Clasificación de conceptos

Instrucción: Relaciona cada concepto con su definición.

Concepto	Definición
a. Activo de información	( ) Debilidad que puede ser explotada por una amenaza.
b. Amenaza	( ) Medida para reducir un riesgo.
c. Vulnerabilidad	( ) Evento potencial que causa daño a un activo.
d. Control	( ) Todo aquello que tiene valor para la organización.

Caso

Una empresa detecta que un empleado abrió un correo con un archivo sospechoso. El antivirus reporta actividad anómala en el equipo. Se teme que datos sensibles de clientes hayan sido expuestos.

Actividad

- Identificar los activos comprometidos.
- Describir la amenaza.
- Evaluar impacto y probabilidad.
- Proponer un plan de tratamiento inmediato.

Activo afectado	Amenaza	Impacto	Probabilidad	Acción inmediata
PC Empleado	Malware (phishing)	Alto	Media	Aislar de red, adquirir imagen de memoria/disco, bloqueo temporal de cuenta
Credenciales del empleado	Robo de credenciales	Alto	Media	Forzar cambio de contraseña, revocar tokens/sesiones, activar MFA
BD de clientes	Exfiltración de datos	Alto	Baja	Revisar logs, consultas inusuales, DLP, cortar accesos anómalos
Gateway de correo	Filtros débiles	Medio	Alta	Endurecer políticas, activar/quebrar macros, revisar DMARC/SPF/DKIM

Ejercicio 3: Mini caso – ¿Qué controla el SGSI?

Situación:

Una empresa sufre un ataque de ransomware. Sus archivos son cifrados y no tienen backups recientes. La dirección decide implementar ISO 27001.

Preguntas:

¿Qué activos se afectaron en este caso?

¿Qué controles hubieran reducido el impacto?

Activo	Tipo	Clasificación

Activos afectados – Mini caso ransomware

Activo	Tipo	Clasificación
Archivos de clientes	Información	Crítico / Confidencial
Servidores de archivos	Hardware/Software	Crítico / Sensible
Información financiera	Información	Confidencial / Sensible
Reputación de la empresa	Intangible	Crítico

Controles del SGSI relevantes (ISO 27001 Anexo A)

A5. Controles Organizacionales

A.5.24 Gestión de incidentes: Procedimientos claros para aislar, responder y recuperar.

A6. Controles de personas

A.6.3 Conciencia de seguridad de la información, educación y formación: Formación en phishing y buenas prácticas.

A8. Controles tecnológicos

A.8.13 Copias de seguridad: Backups regulares y pruebas de restauración.

A.8.7 Protección contra malware: Antivirus, EDR, monitoreo en tiempo real.

A.8.9 Gestión de la configuración: Actualización continua de sistemas y aplicaciones.

Referencias

1. Bishop, M. (2003). *Computer Security.*
2. Briceño, E. (2021). *Seguridad De La Información*
3. Kremer, E. Et al. (2019). *Ciberseguridad*
4. Ozkaya, E. (2019). *Cybersecurity: The Beginner's Guide: A comprehensive guide to getting started in cybersecurity*
5. *NORMA TÉCNICA NTC-ISO-IEC COLOMBIANA 27001*
6. *General Data Protection Regulation (GDPR)*
7. LEY ESTATUTARIA 1581 DE 2012. *Link: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981*