UNIVERSIDAD SERGIO ARBOLEDA | Colsubsidio

Diplomado de Ciberseguridad y Gestión de Seguridad de la Información

Módulo 3:

Regulación de la Seguridad de la Información y Protección de Datos

Sesión 2:

Aplicación práctica: diseño de políticas básicas

OBJETIVO DE LA SESIÓN:

Aplicar los conceptos de regulación para diseñar políticas básicas de protección de datos y seguridad de la información.


MAYOR
FILTRACIÓN
DE LA HISTORIA

Problemas por falta de políticas claras

Caso Sony Pictures (2014)

Qué pasó: Hackers robaron correos internos y películas sin estrenar.
Causa: No había una política estricta sobre gestión de contraseñas y segmentación de accesos. Muchos empleados usaban claves débiles (“password123”).
Problema: La información interna y privada de empleados quedó expuesta.

Imagen Tomada de 11

¿Qué política faltaba?

¿Qué impacto tuvo (económico, reputacional, legal)?

¿Qué control habría evitado el incidente?

Lecciones Aprendidas

Medidas básicas de seguridad son cruciales

- Monitoreo de red, detección de amenazas y gestión de parches
- Filtros de correo y firewalls
- Políticas de retención de correos

Protección reforzada de datos sensibles

- Cifrado y almacenamiento seguro
- Control de acceso y autenticación multifactor
- Segmentación de redes + copias de seguridad

Plan de respuesta a incidentes es vital

- Protocolos claros para continuar operaciones
- Pruebas de penetración y simulacros periódicos

Problemas por falta de políticas claras

Caso Equifax (2017)

Qué pasó: Filtración de datos de 147 millones de personas (SSN, direcciones, tarjetas).
Causa: No había una política clara de actualización de sistemas. Un fallo conocido en Apache Struts no fue parchado a tiempo.
Problema: Los atacantes explotaron esa vulnerabilidad durante meses.

Imagen Tomada de 9

¿Qué política faltaba?

¿Qué impacto tuvo (económico, reputacional, legal)?

¿Qué control habría evitado el incidente?

Lecciones Aprendidas

Centrarse en lo básico
- Parcheo oportuno de vulnerabilidades
- Renovación de certificados de seguridad

Segmentación de red es clave
- Limita la superficie de ataque
- Facilita la contención en caso de brecha

Implementar arquitectura Zero Trust
- Acceso mínimo necesario a datos sensibles
- Monitorización rigurosa de accesos y privilegios
- Detección temprana de intentos de exfiltración

Problemas por falta de políticas claras

Caso de la ciudad de Oslo: Exposición de datos de residencias de ancianos

Qué pasó: La Ciudad de Oslo almacenó hojas de trabajo electrónicas con datos personales de residentes de hogares de ancianos fuera del sistema electrónico oficial de salud, entre 2007 y 2018.
Causa: La Ciudad de Oslo almacenó hojas de trabajo electrónicas con datos personales de residentes de hogares de ancianos fuera del sistema electrónico oficial de salud, entre 2007 y 2018.
Problema: Miles de datos personales quedaron accesibles a personal no autorizado sin registro de acceso ni supervisión adecuada.

Imagen Tomada de 10

¿Qué política faltaba?

¿Qué impacto tuvo (económico, reputacional, legal)?

¿Qué control habría evitado el incidente?

Lecciones Aprendidas

Control de acceso estricto
- Implementar roles y permisos diferenciados
- Evitar accesos innecesarios a datos sensibles

Almacenamiento seguro de datos
- Centralizar la información en sistemas oficiales
- Prohibir el uso de archivos externos no controlados

Auditoría y supervisión continua
- Monitorear quién accede a los datos y con qué propósito
- Revisar periódicamente la seguridad de la información

Capacitación del personal
- Sensibilizar sobre el manejo responsable de datos
- Promover buenas prácticas de protección de información crítica

¿Qué es una política de seguridad de la información?

Una política de seguridad de la información es un documento formal emitido por la alta dirección de una organización, que establece:

- Su **compromiso** con la seguridad de la información.
- Las **directrices generales** para proteger los activos de información.
- El **marco de referencia** para definir objetivos, controles y procedimientos específicos.

Definición según ISO/IEC 27001:2022

La norma define en su **cláusula 5.2 (Política)** que:
La organización debe establecer una **política de seguridad de la información** que:

- Sea adecuada al propósito de la organización.
- Incluya compromisos para satisfacer requisitos aplicables y mejorar continuamente el SGSI.
- Proporcione un marco para establecer objetivos de seguridad de la información.
- Se comunique dentro de la organización.
- Esté disponible para partes interesadas relevantes, según corresponda.

En palabras simples:
Es un documento donde la organización declara:

- "Para nosotros la seguridad de la información es importante."
- "Este es el camino que seguiremos para proteger nuestros datos y los de nuestros clientes."
- "Así garantizamos confidencialidad, integridad y disponibilidad."

¿Por qué es necesaria?

1. Define reglas claras para todos.

- **Ejemplo:** Prohibición de compartir contraseñas o requisitos mínimos para claves seguras.

2. Es la base del Sistema de Gestión de Seguridad de la Información (SGSI).

- Sin política no hay marco formal para controles, objetivos y auditorías.

3. Demuestra compromiso de la alta dirección.

- Requisito clave en auditorías ISO/IEC 27001:2022.

Componentes clave según ISO/IEC 27001:2022

Aunque la norma no impone un formato único, sugiere que la política incluya:

Componente	Explicación práctica
Propósito	¿Por qué existe esta política? Ej. Proteger información de clientes, empleados y socios.
Alcance	Áreas, procesos, personas y sistemas a los que aplica. Ej. Toda la organización y proveedores críticos.
Compromisos	Declaraciones de la dirección sobre: – Cumplimiento legal y contractual– Mejora continua del SGSI– Gestión de riesgos
Principios generales	Confidencialidad, integridad, disponibilidad, y cualquier principio de seguridad aplicable.
Roles y responsabilidades	Quién es responsable de implementar, mantener y revisar la política.
Comunicación	Cómo se comunicará y mantendrá actualizada. Ej. Publicada en intranet, comunicada en inducciones y capacitaciones.

Ejemplo práctico resumido

Política de Seguridad de la Información

La empresa X declara su compromiso con la seguridad de la información para proteger los datos de empleados, clientes y socios, garantizando su confidencialidad, integridad y disponibilidad.
Esta política aplica a todos los colaboradores, contratistas y proveedores que accedan a los sistemas o datos de la organización.
La dirección se compromete a cumplir las leyes aplicables y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).
Todos los empleados deben:

- ***Usar contraseñas fuertes y no compartirlas.***
- ***Reportar incidentes de seguridad inmediatamente.***

El Oficial de Seguridad de la Información será responsable de su implementación y revisión anual.

Claves de la ISO/IEC 27001:2022 sobre la política

La política NO describe todos los controles específicos, sino las **directrices generales**.

Es el **punto de partida** para crear procedimientos más detallados.
Ejemplo: La política dice “proteger datos personales”; el procedimiento define cómo (ej. cifrado, permisos, backups).

Es revisada y aprobada por la **alta dirección**, no solo por el área de TI o seguridad.

Imagina que la política es el reglamento general de un colegio.
Define valores, normas básicas y responsabilidades para todos.
Luego, cada clase (procedimiento) desarrolla actividades específicas, pero siempre alineadas al reglamento general.

Ejercicio 1: Construcción Guiada de Política

En grupos, construyan una política básica de seguridad de la información para el siguiente escenario, **siguiendo los requisitos de la norma ISO/IEC 27001:2022 (cláusula 5.2).**

Una plataforma virtual de tutorías recolecta información de estudiantes (nombre, edad, correo) y docentes (cédula, correo, estudios). La dirección desea implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** y como primer paso necesita su política.

Aspectos que deben incluir en la política (alineados con ISO/IEC 27001:2022)

Propósito de la política (Propósito/Objetivo)
– ¿Por qué se crea esta política?
Alcance (Ámbito de aplicación)
– ¿A quiénes y a qué procesos o sistemas aplica?
Compromisos de la dirección
– Cumplir requisitos aplicables (legales, regulatorios, contractuales)
– Mejorar continuamente el SGSI

Principios generales de seguridad de la información
– Confidencialidad, integridad, disponibilidad, y cualquier otro aplicable
Roles y responsabilidades clave
– Ej. Responsable de Seguridad de la Información
Comunicación y revisión
– ¿Cómo se comunicará y revisará esta política?

Ejercicio 2: Socialización: Presentación de la política diseñada

Cada grupo presentará su política de seguridad de la información y protección de datos creada en el ejercicio anterior.
Deben explicar brevemente:

1. Su propósito.
2. Alcance y ámbito de aplicación.
3. Compromisos de la dirección.
4. Principios generales.
5. Roles y responsabilidades.
6. Cómo planean comunicarla y revisarla.

El escándalo de Cambridge Analytica

Ejercicio 3: Debate breve: Cumplimiento legal vs. responsabilidad ética

¿Es más importante cumplir la ley o proteger éticamente la información de las personas? ¿Por qué?

una app que comparte datos médicos con farmacéuticas aunque los usuarios lo autorizaron en los términos y condiciones.

un empleado descarga datos porque no está prohibido en la política, pero igual causa un incidente.

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*
8. Imagen Noticias*. (2025) La mayor filtración de datos en la historia: exponen 16 mil millones de contraseñas y nombres | NL https://www.youtube.com/watch?v=KD2xM7cqMK4&t=2s*
9. Breachsense. (2024, diciembre 8). . *Equifax data breach case study: Causes and aftermath. Breachsense.com, https://www.breachsense.com/blog/equifax-data-breach/*
10. The Norwegian Data Protection Authority imposes a fine on the City of Oslo. (2019, diciembre 18). *Europa.eu., https://www.edpb.europa.eu/news/national-news/2019/norwegian-data-protection-authority-imposes-fine-city-oslo_ro*
11. *Young, K. (2021, noviembre 8). Cyber case study: Sony Pictures Entertainment hack. CoverLink Insurance - Ohio Insurance Agency; CoverLink Insurance. https://coverlink.com/case-study/sony-pictures-entertainment-hack/*
12. *Efecto Naim. (2018). El escándalo de Cambridge Analytica en 5 minutos. https://www.youtube.com/watch?v=PUvsowKJGkY*