

Actividad: Desarrollo de Políticas y Procedimientos de Seguridad

Objetivo:

Desarrollar y aplicar políticas de seguridad informática, crear procedimientos de respuesta a incidentes, y diseñar estrategias de gestión de riesgos y cumplimiento normativo.

Parte 1: Políticas y Procedimientos de Seguridad

Instrucciones:

1. Investigación Inicial:

- **Objetivo:** Comprender la importancia de las políticas de seguridad y su aplicación en la protección de sistemas y datos.
- **Actividad:**
 1. Investiga qué son las políticas de seguridad informática y por qué son fundamentales para cualquier organización.
 2. Redacta una breve descripción de los componentes esenciales de una política de seguridad (por ejemplo, control de acceso, protección de datos, uso aceptable de recursos).
 3. Revisa las políticas de seguridad de una empresa real (puedes buscar ejemplos en línea) y analiza cómo se estructuran.

2. Desarrollo de una Política de Seguridad:

- **Objetivo:** Crear una política de seguridad básica para una pequeña empresa ficticia.
 - **Actividad:**
 1. Imagina que estás desarrollando una política de seguridad para una pequeña empresa de tecnología. Define los siguientes aspectos:
 - **Control de acceso:** ¿Quiénes tienen acceso a qué recursos y bajo qué condiciones?
 - **Protección de datos:** ¿Cómo se protegerán los datos sensibles de la empresa?
 - **Gestión de contraseñas:** ¿Qué requisitos de complejidad y cambio de contraseñas se establecerán?
 - **Uso aceptable de recursos:** ¿Qué comportamientos se permitirán o prohibirán en el uso de los recursos tecnológicos de la empresa?
 2. Documenta la política en un informe breve y estructurado.
-

Parte 2: Estrategias de Gestión de Riesgos y Cumplimiento Normativo

Instrucciones:

1. Análisis de Riesgos:

- **Objetivo:** Identificar y analizar los riesgos de seguridad informática que enfrenta una organización.
 - **Actividad:**
 1. Define qué es la gestión de riesgos en el contexto de la seguridad informática.
 2. Elige tres posibles riesgos de seguridad para la empresa ficticia mencionada anteriormente (por ejemplo, ataques de malware, brechas de datos, o acceso no autorizado).
 3. Evalúa cada riesgo en términos de probabilidad de ocurrencia y posible impacto, usando una matriz de riesgos.
 - 2. **Cumplimiento Normativo:**
 - **Objetivo:** Entender las normativas de seguridad y cómo asegurar que la empresa cumple con ellas.
 - **Actividad:**
 1. Investiga una normativa de seguridad relevante (por ejemplo, GDPR, ISO 27001) y describe brevemente sus requisitos clave.
 2. Sugiere cómo la empresa ficticia podría implementar cambios para cumplir con dicha normativa.
-

Parte 3: Creación de Procedimientos de Respuesta a Incidentes

Instrucciones:

1. **Procedimientos de Respuesta:**
 - **Objetivo:** Desarrollar un plan de respuesta a incidentes de seguridad.
 - **Actividad:**
 1. Define qué es un incidente de seguridad y da ejemplos de posibles incidentes (por ejemplo, ataque de ransomware, phishing).
 2. Desarrolla un procedimiento paso a paso que la empresa ficticia debería seguir en caso de un ataque de malware:
 - **Detección:** ¿Cómo se detectaría el incidente?
 - **Contención:** ¿Qué medidas inmediatas se tomarían para limitar el daño?
 - **Erradicación:** ¿Cómo se eliminaría la amenaza?
 - **Recuperación:** ¿Cómo se restaurarían los sistemas afectados?
 - **Lecciones aprendidas:** ¿Qué se podría hacer para evitar que el incidente se repita?
-

Conclusión:

- Al finalizar, prepara un breve informe que incluya:
 1. Un resumen de la política de seguridad desarrollada.
 2. Los resultados del análisis de riesgos y las medidas para cumplir con la normativa.

3. El procedimiento de respuesta a incidentes.
4. Reflexiona sobre la importancia de la seguridad informática en las empresas modernas.