Actividad práctica: Análisis de seguridad en un entorno empresarial

Duración: 2 horas de preparación, más exposición de 10-15 minutos.
Objetivo: Identificar vulnerabilidades, clasificar medidas de seguridad y plantear soluciones frente a incidentes.
Formato: Trabajo en grupos de tres alumnos y posterior exposición.

TechnoCorp es una empresa mediana del sector tecnológico con 15 empleados distribuidos en un único edificio de oficinas. Su actividad principal consiste en ofrecer servicios de consultoría informática y desarrollo de software para pymes. Dispone de una red interna que conecta todos los equipos de la oficina, así como un servidor local que almacena información sensible de clientes, proyectos en curso y facturación. Además, cuenta con una red WiFi para empleados y otra para visitas, aunque no siempre se gestiona correctamente.

La empresa realiza operaciones frecuentes de comercio electrónico, como la compra de licencias y componentes informáticos, y gestiona pagos electrónicos tanto con proveedores como con clientes. Los equipos de sobremesa y portátiles son utilizados diariamente por el personal, que en muchos casos no tiene formación en seguridad informática. No existe un departamento dedicado exclusivamente a seguridad, y las medidas aplicadas son básicas: un antivirus genérico, contraseñas simples y copias de seguridad poco sistemáticas.

Entre los activos críticos se encuentran el servidor de archivos, la base de datos de clientes, los portátiles de la gerencia y la reputación de la empresa frente a sus clientes. TechnoCorp es consciente de que un fallo de seguridad podría afectar gravemente su continuidad, bien sea por una pérdida de información, un ataque de denegación de servicio o un fraude en línea. Actualmente, la dirección quiere reforzar la protección de sus sistemas, pero carece de un plan de seguridad formal y espera que los nuevos responsables puedan identificar riesgos, proponer medidas y establecer políticas claras que garanticen la confidencialidad, la integridad y la disponibilidad de la información.

Fase 1 – Análisis inicial (20 min)

Tarea:

1. Identificar **activos críticos** (hardware, software, información, personal).
2. Anotar posibles **amenazas** para cada activo.
3. Clasificarlas como **seguridad física/lógica** y **activa/pasiva**.

Fase 2 – Estudio de incidentes (30 min)

Tarea:

- Determinar **qué principios de seguridad** se vulneran (Confidencialidad, Integridad, Disponibilidad, No repudio).
- Proponer una **medida preventiva** y una **medida correctiva** para cada caso.

Fase 3 – Priorización de riesgos (30 min)

| Amenaza | Vulnerabilidad | Valor del bien | Nivel de riesgo (B/M/A) | Medida recomendada |

Ejemplos:

- Inundación en sala de servidores.
- Ataque DoS a la web corporativa.
- Robo de portátil de un directivo.

Tarea:

- Generar la tabla con las siguientes columnas:
  | Amenaza | Vulnerabilidad | Valor del bien | Nivel de riesgo (B/M/A) | Medida |
- Completar la tabla con los anteriores ejemplos, y asignando un nivel de riesgo y una medida.
- Priorizar los riesgos de mayor impacto.

Fase 4 – Presentación y discusión (30 min + 15 min)

Cada grupo presenta en **10 -15 minutos**, con las siguientes partes:

- Explicación de las tres fases trabajadas: Análisis Inicial, Estudio de Incidentes y Priorización de Riesgos.
- Medidas clave de seguridad física y una lógica.
- Recomendaciones generales para la dirección de la empresa.