Actividad Evaluable (E2)

DESCRIPCIÓN GENERAL DE LA PRÁCTICA:

Esta actividad evaluable consiste en:

Ejercicio 1. Plan de seguridad.

Elabora un documento explicando que es un Plan de Seguridad Informática y los pasos a seguir para su elaboración.

Ejercicio 2. Coste de un incidente: Robo de Dispositivos Móviles.

***Contexto*:** Varios dispositivos móviles corporativos han sido robados, conteniendo información sensible. El BIA determina que el impacto por cada día que la información pueda estar expuesta es de 1500€. El personal de seguridad considera tres posibles estrategias para mitigar el impacto:

a. Activar el borrado remoto de los dispositivos, lo que tomará 1 día. El coste es de 500€.
b. Implementar una solución de gestión de dispositivos móviles (MDM) para evitar futuras incidencias, lo que tomará 3 días. El coste es de 4000€.
c. Realizar un seguimiento de los dispositivos y recuperarlos, lo que tomará 5 días. El coste es de 1000€.
d. Calcula el coste de cada una de las opciones e indica los pros y contras de cada una de las mismas.

Ejercicio 1. Plan de seguridad

Un ***Plan de Seguridad Informática*** es un documento que establece las directrices y acciones para proteger a la infraestructura tecnológica, datos e información de una organización contra amenazas y vulnerabilidades. ***El objetivo*** de este Plan es garantizar la confidencialidad, integridad y

disponibilidad de la información, asegurando además, la continuidad del negocio en caso de que haya incidentes de seguridad.

Su ***importancia*** es la siguiente:

1. **Protección de Datos**: Asegurar la protección de datos sensibles y críticos.
2. **Cumplimiento Normativo**: Garantizar el cumplimiento de leyes y regulaciones.
3. **Prevención de Ataques**: Minimizar el riesgo de ciberataques y posibles impactos.
4. **Continuidad del Negocio**: Establecer protocolos para mantener las operaciones en caso de incidentes.
5. **Reputación**: Proteger la reputación de la organización para evitar brechas de seguridad.

Los pasos para seguir la ***Elaboración del Plan de Seguridad Informática***:

1. **Evaluación Inicial**:
    a. **Inventario de Activos**: Identificar y catalogar todos los activos tecnológicos y datos.
    b. **Análisis de Riesgos**: Evaluar las amenazas y vulnerabilidades, así como el impacto potencial de cada una.
    c. **Clasificación de Datos**: Categorizar los datos según su nivel de sensibilidad y valor para la organización.

2. **Definición de Políticas y Procedimientos**:
    a. **Políticas de Seguridad**: Desarrollar políticas claras que aborden el uso aceptable de recursos, gestión de contraseñas, acceso a datos, etc.
    b. **Procedimientos de Seguridad**: Establecer procedimientos específicos para implementar y mantener las políticas de seguridad.

3. **Desarrollo de un Plan de Respuesta a Incidentes**:
    a. **Equipos de Respuesta**: Designar un equipo responsable de la respuesta a incidentes de seguridad.

   b. **Protocolos de Respuesta**: Definir procedimientos claros para identificar, contener, erradicar y recuperar de incidentes de seguridad.
   c. **Comunicación**: Establecer un plan de comunicación interna y externa en caso de incidentes.

4. **Implementación de Controles de Seguridad**:
   a. **Controles Técnicos**: Implementar medidas como firewalls, sistemas de detección de intrusos, cifrado de datos, etc.
   b. **Controles Físicos**: Asegurar la infraestructura física, como los centros de datos y oficinas.
   c. **Controles Administrativos**: Definir roles y responsabilidades claras, realizar capacitaciones y concienciar a los empleados.

5. **Monitoreo y Mantenimiento**:
   a. **Monitoreo Continuo**: Utilizar herramientas de monitoreo para detectar y responder a las actividades sospechosas en tiempo real.
   b. **Revisiones Periódicas**: Realizar auditorías y revisiones periódicas del plan para asegurar su efectividad y hacer ajustes necesarios.
   c. **Actualizaciones**: Mantener el plan actualizado frente a nuevos riesgos y tecnologías emergentes.

6. **Capacitación y Concienciación**:
   a. **Programas de Capacitación**: Desarrollar programas de formación para todos los empleados sobre prácticas de seguridad.
   b. **Concienciación Continua**: Implementar campañas de concienciación para mantener la seguridad como una prioridad constante.

7. **Evaluación y Mejora Continua**:
   a. **Pruebas y Simulacros**: Realizar pruebas y simulacros de los planes de respuesta a incidentes para evaluar la preparación.
   b. **Retroalimentación**: Recopilar retroalimentación de incidentes y pruebas para identificar áreas de mejoras.
   c. **Actualización del Plan**: Revisar y actualizar el plan regularmente para adaptarse a cambios en el entorno de seguridad.

Ejercicio 2. Coste de un incidente: Robo de Dispositivos móviles

Su impacto diario por la exposición de la información (1500€/día):

a. **Coste Solución A (Activar el Borrado Remoto de los Dispositivos, 1 día):**
    - Tiempo: 1 día
    - Coste de implementación: 500€
    - Coste del impacto: 1 x 1500 = 1500€

Costo total: 500 + 1500 = 2000€

b. **Coste Solución B (Implementar una Solución de Gestión de Dispositivos Móviles [MDM], 3 días):**
    - Tiempo: 3 días
    - Coste de implementación: 4000€
    - Coste del impacto: 3 x 1500 = 4500€

Costo total: 4000 + 4500 = 8500€

c. **Coste Solución C (Realizar un Seguimiento de los Dispositivos y Recuperarlos, 5 días):**
    - Tiempo: 5 días
    - Coste de implementación: 1000€
    - Coste del impacto: 5 x 1500 = 7500€

Costo total: 1000 + 7500 = 7500€

PROS Y CONTRAS DE CADA COSTE DE SOLUCIÓN:

a. **Activar el Borrado Remoto de los Dispositivos:**
    - *PROS*:
        - Rápida implementación (1 día).
        - Coste de implementación relativamente bajo (2000 €).
    - *CONTRAS*:
        - Información perdida permanentemente.

        - No proviene de futuros robos o incidentes similares.

b. **Implementar una Solución de Gestión de Dispositivos Móviles [MDM]:**
    - *PROS*:
        - Solución a largo plazo para prevenir futuras incidencias.
        - Mejora la gestión y seguridad de todos los dispositivos móviles de la empresa.
        - Potencial para más funcionalidades de seguridad y administración de dispositivos.
    - *CONTRAS*:
        - Mayor tiempo de implementación (3 días).
        - Coste de implementación alto (8500 €).
c. **Realizar un Seguimiento de los Dispositivos y Recuperarlos:**
    - *PROS*:
        - Posibilidad de recuperar tanto los dispositivos como la información contenida.
        - Coste de implementación relativamente bajo (1000 €).
    - *CONTRAS*:
        - Mayor tiempo de exposición de la información (5 días).
        - Alto riesgo de no recuperar los dispositivos.
        - Mismo coste que la **opción B (Implementar una Solución de Gestión de Dispositivos Móviles [MDM])** pero sin las ventajas de una solución preventiva.

Para elegir una opción dependerá de la urgencia de la situación, presupuesto disponible y prioridad que se le dé a la prevención a largo plazo frente a la resolución inmediata del problema actual, ya que:

1. La **opción A** es la más rápida y económica a corto plazo, adecuada para la solución inmediata a la exposición de la información.
2. La **opción B** es costosa pero ofrece una solución a largo plazo que puede prevenir futuros incidentes y así mejorar la seguridad general de la empresa.
3. La **opción C** tiene un coste de implementación bajo pero es arriesgado debido al largo tiempo de exposición y la incertidumbre de recuperar todos los dispositivos.