Actividad 5 – Analiza la seguridad de la información en una empresa

Pol de la Viuda

Contenido

Parte 1 – Comprensión teórica

¿Qué es una política de seguridad y cuál es su principal objetivo dentro de una organización?

Una política de seguridad es un conjunto de normas y medidas que se aplican en una empresa para proteger su información y sus sistemas. Su objetivo principal es evitar problemas como robos de datos, accesos no autorizados o pérdidas de información importante.

Nombra dos herramientas que se utilizan para el análisis y gestión de riesgos e indica brevemente para qué sirven.

- OCTAVE: Sirve para identificar los riesgos que pueden afectar a los sistemas informáticos y planificar cómo reducirlos.
- MAGERIT: Ayuda a analizar los riesgos y proponer medidas de seguridad adecuadas, muy usada en la administración pública.

¿Qué diferencia hay entre una auditoría total y una auditoría parcial?

La auditoría total revisa todo el sistema de una empresa, mientras que la parcial se centra solo en una parte concreta, como la red, los servidores o las contraseñas de los empleados.

Explica con tus palabras qué es un plan de contingencias y cuáles son sus tres subplanes principales.

Un plan de contingencias es un conjunto de pasos que se siguen cuando ocurre un problema grave, como una caída del sistema o una pérdida de datos.
Sus tres partes principales son:

- Respaldo: Hacer copias de seguridad.
- Emergencia: Actuar rápido cuando ocurre el problema.
- Recuperación: volver a la normalidad lo antes posible.

De los modelos de seguridad (Matriz de acceso, RBAC, Multinivel), elige uno y explica cómo se aplicaría en un centro educativo o empresa.

El modelo RBAC (Control de Acceso Basado en Roles) asigna permisos

según el puesto de cada persona.
Por ejemplo, en un instituto: los profesores pueden editar notas, los alumnos solo verlas y el personal de administración tiene acceso a todo el sistema. Así se evita que alguien acceda a información que no le corresponde.

Parte 2 – Caso Practico

Informe de política de seguridad

Para evitar caídas del servidor como la que ocurrió, se deberían aplicar medidas como: copias de seguridad automáticas, control de accesos por roles, mantenimiento regular del sistema y monitorización constante de los servidores. Además, sería recomendable tener un plan de respuesta rápida ante incidentes.

Auditoría parcial

Activos a revisar

- Servidor principal.
- Base de datos de clientes.
- Equipos de red (switches, routers).
- Políticas de acceso y contraseñas de los empleados.

Herramientas

- Nessus: Para detectar vulnerabilidades.
- Wireshark: Para analizar el tráfico de red.
- OCS Inventory: Para registrar y controlar los equipos.

Plan de Contingencia Básico

Respaldo: Copias de seguridad diarias en la nube y una copia semanal en un disco externo

Emergencia: Avisar al responsable de sistemas y activar un servidor alternativo si el principal falla

recuperación: Restaurar los datos desde la copia mas reciente y comprobar que todo funcione correctamente

Modelo de seguridad aplicado

Usaría el modelo RBAC, donde cada trabajador tiene permisos según su función:

- Los administradores pueden gestionar todo.
- Los técnicos solo acceden al mantenimiento.
- El personal de oficina solo puede consultar los datos necesarios.

Esto evita errores humanos y accesos indebidos a información sensible.

Parte 3 – Creatividad

Infografía