PARTE 2 POLÍTICAS DE ALMACENAMIENTO Y CARACT DE DISPOSI

PARTE 3

3.1. Análisis completo de incidente de seguridad

Lee el siguiente escenario:

Una empresa detecta que varios empleados reciben correos con facturas adjuntas. Una de ellas contiene un malware que cifra los archivos del servidor.
El servidor tenía RAID 1, pero las copias de seguridad estaban en un pendrive que se guardaba en un cajón. El responsable de TI descubre que el pendrive lleva dos semanas sin actualizarse y que además no estaba cifrado.
Tras el incidente, los datos personales de clientes quedan inaccesibles durante 48 horas.

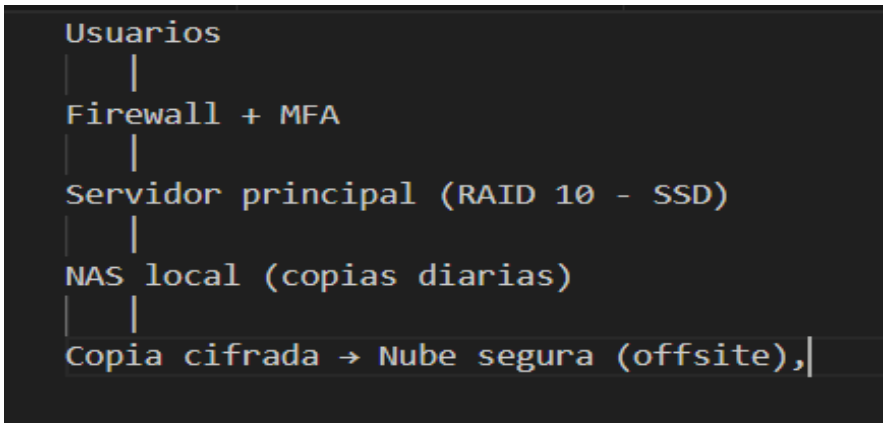
Responde:

a) Identifica **todas las amenazas** presentes (mínimo 4).
Las amenazas que tiene son la falta de cifrado, amenazas de Phishing, la perdida de copias de seguridad si se pierde el pendrive y malware.
b) ¿Qué **fallos de política de almacenamiento** se observan?
Los fallos de política que observo son: que no tienen copias automatizadas ni semanales, no tienen cifrado de datos y tener solo un pendrive como solución a perdidas futuras.
c) ¿Qué artículos del **RGPD** podrían haberse incumplido?
El artículo del RGPD que podrían haberse saltado es: Artículo 5 Artículo 25 y Artículo 32
d) ¿Qué medidas técnicas y organizativas deberían implantarse?
La técnicas que deberían implantarse son:
e) ¿Cómo habría cambiado el resultado si la empresa usara:

- Copias remotas en la nube: podrían haber recuperado rápidamente los datos, no tener información perdida.
- Un plan 3-2-1: Podría haber protegido mejor el ransomware, y podrían continuar después de un fallo al momento.
- Cifrado + autenticación multifactor: podrían haber protegido la información del pendrive robado podrían haber hecho el cumplimiento de RGPD.

3.2. Diseño de arquitectura segura de almacenamiento

Diseña para una empresa mediana un sistema completo que incluya:



La elección de dispositivos seria SSD en RAID 10 porque es más rápido, las copias de seguridad serian diariamente y de tipo diferencial, las versiones que se conservarían serian de cada mes, los datos estarían en reposos y en transito

Fuera del edificio se pondrían los datos en la nube y se garantizaría la disponibilidad con un SAI 24/7

Deben presentarlo en forma de diagrama + explicación de 8–12 líneas.

3.3. Análisis de coste–beneficio

La empresa dispone de dos opciones:

Opción A:

- RAID 1 local
- Copias semanales en HDD externo
- Sin nube
- Coste: 300 €/año
- Riesgo de pérdida total: medio

Opción B:

- RAID 5
- Copias diarias en la nube cifrada
- Monitorización automática
- Coste: 1.200 €/año
- Riesgo de pérdida total: muy bajo

Responde:

a) ¿Qué opción es mejor a largo plazo?

La mejor opción es la opción B

b) ¿En qué casos conviene la opción A?

El caso A es el mejor en empresas pequeñas, para datos que no sean críticos y presupuesto bajo.

c) ¿Qué impacto tendría en disponibilidad, recuperación y cumplimiento del RGPD?

	Caso A	Caso B
Disponibilidad	Impacto medio	Impacto Alto
Recuperación	Lenta	Rápida
RGPD	Riesgo de incumplimiento	Cumplimiento

3.4. Escenario de continuidad de negocio

Imagina que un incendio destruye totalmente la oficina donde están los servidores.

Explica:

a) Qué pasaría si la empresa solo usara RAID.

Si el usuario solo utilizara RAID Los datos estarían perdidos

b) Qué pasaría si la empresa usara copias locales, pero no remotas.

Podrían destruirse por causas físicas como inundaciones fuego y se perdería toda la información

c) Qué pasaría si aplicara el método 3-2-1 correctamente.

Lo que pasaría seria que la copias de seguridad estarían intactas que la restauración seria desde la nube y si algo falla todo seguiría funcionando.

d) Tiempo estimado de recuperación en cada caso (cuantifícalo).

Caso	Tiempo
Solo RAID	No se podrían recuperar
Copias locales	No se podrían recuperar
3-2-1	1-3 días

e) Redacta un mini plan de recuperación (5 líneas). El plan de recuperación seria activar el plan de recuperación, acceder a copias remotas también verificar la integridad de los datos y comunicar el incidente a clientes y auditorias para poder mejorar el plan de seguridad y mantener informados de errores

3.5. Evaluación de dos escenarios de almacenamiento

Compara y elige la mejor solución:

Empresa 1:

- Trabaja con video 4K
- Necesita mucha velocidad
- Ficheros enormes
- Poco crítico si se pierde algo
  → Opciones: SSD NVMe / HDD / RAID 0
- La mejor opción es usar SSD NVMe ya que te da una alta velocidad de lectura y escritura también porque ofrece mayor rendimiento que HDD
-

Empresa 2:

- Datos financieros sensible
- Información personal
- Alta disponibilidad
- Prohibida la pérdida de datos
  → Opciones: RAID 6 / RAID 10 / nube cifrada
- La mejor opción es RAID 10 ya que combina redundancia y buen rendimiento cosa que permite fallos de discos sin la perdida de datos y ofrece mejor tiempo de recuperación que RAID 6

Explica tu elección para cada caso y justifícala bien.