Alejandro Molina de haro

16/12/2025

Parte 2 Políticas de Almacenamiento y Caract de Disposi

Tabla de contenido

3.1. Análisis completo de incidente de seguridad

a) Amenazas presentes

En este caso se pueden identificar varias amenazas.
La primera es el **phishing**, ya que los trabajadores reciben correos falsos con facturas adjuntas.
También hay **malware o ransomware**, porque uno de esos archivos infecta el sistema y cifra los datos del servidor.
Otra amenaza importante es la **pérdida de disponibilidad**, ya que los datos de los clientes están inaccesibles durante 48 horas.
Además, las **copias de seguridad no son seguras**, porque se guardaban en un pendrive sin cifrar.
También se aprecia un **error humano**, ya que el pendrive llevaba dos semanas sin actualizarse.
Por último, existe **riesgo de fuga de datos**, porque si alguien accede al pendrive podría ver información personal.

b) Fallos en la política de almacenamiento

Uno de los principales fallos es pensar que **usar RAID es lo mismo que tener copias de seguridad**, cuando no es así.
Las copias se hacían **de forma manual**, por lo que no estaban siempre actualizadas.
Solo se utilizaba **un único dispositivo** para las copias, que además era un pendrive.
Las copias **no estaban cifradas**, lo que supone un riesgo grave.
Tampoco se aplicaba el **método 3-2-1**.
Además, no se realizaban **comprobaciones ni controles periódicos** de las copias.

c) Artículos del RGPD posiblemente incumplidos

Se podría haber incumplido el **artículo 5.1.f**, que exige garantizar la integridad y confidencialidad de los datos.
También el **artículo 32**, que obliga a aplicar medidas de seguridad adecuadas.
El **artículo 25** puede no haberse cumplido, ya que no se tuvo en cuenta la protección de datos desde el diseño.
Además, si el incidente supuso un riesgo para los datos personales, debería aplicarse el **artículo 33**, sobre la notificación de brechas de seguridad.

d) Medidas técnicas y organizativas

Medidas técnicas:

- Realizar **copias de seguridad automáticas y cifradas**.
- Guardar copias **en la nube o en una ubicación externa**.
- Usar **antivirus y filtros de correo** para evitar archivos maliciosos.
- Aplicar **control de accesos y autenticación multifactor** .
- Separar la red para evitar que el malware se propague.

Medidas organizativas:

- Establecer una **política clara de copias de seguridad**.
- Dar **formación a los empleados** sobre correos peligrosos.
- Realizar **revisiones periódicas** del sistema.
- Tener un **plan de continuidad y recuperación** ante incidentes.

e) Cómo habría cambiado el resultado si

- **Copias en la nube:** se podrían haber recuperado los datos rápidamente sin depender del servidor afectado.
- **Plan 3-2-1:** existirían varias copias actualizadas, incluyendo una fuera del edificio.
- **Cifrado y MFA:** el malware tendría más dificultades y los datos estarían mejor protegidos.

3.2. Diseño de arquitectura segura de almacenamiento

La empresa utiliza un servidor principal con discos SSD en RAID 10, lo que proporciona buen rendimiento y tolerancia a fallos. Se realizan copias de seguridad incrementales todos los días y copias completas una vez a la semana. Las copias más recientes se almacenan en un NAS local para poder restaurar los datos de forma rápida en caso de fallo. Además, se realizan copias automáticas en la nube, que se guardan fuera del edificio. Estas copias están cifradas para proteger la información. Se conservan hasta 30 versiones de los datos. Los datos están cifrados tanto en reposo como en tránsito. El acceso al sistema está protegido mediante autenticación multifactor. El sistema cuenta con monitorización las 24 horas para detectar problemas. Todo esto permite garantizar una alta disponibilidad y una buena recuperación ante desastres.

3.3. Análisis de coste–beneficio

a) Mejor opción a largo plazo

La mejor opción a largo plazo es la **opción B**, ya que ofrece mayor seguridad, reduce casi por completo el riesgo de pérdida de datos y cumple mejor con el RGPD, aunque su coste sea más alto.

b) Cuándo conviene la opción A

La opción A puede ser adecuada para **empresas pequeñas**, con **datos poco importantes**, que tengan un **presupuesto muy limitado** y que no estén obligadas a cumplir requisitos legales estrictos en cuanto a protección de datos.

c) Impacto en disponibilidad, recuperación y RGPD

La opción A ofrece una **disponibilidad baja**, una **recuperación lenta** en caso de fallo y un **cumplimiento del RGPD deficiente**.
En cambio, la opción B proporciona **alta disponibilidad**, una **recuperación muy rápida** ante incidentes y un **alto nivel de cumplimiento del RGPD**.

3.4. Escenario de continuidad de negocio

a) Solo RAID

Si la empresa solo utilizara RAID y se produjera un incendio, se perderían todos los datos, ya que el RAID no protege frente a desastres físicos. En este caso no sería posible recuperar la información, por lo que el tiempo de recuperación sería imposible.

b) Copias locales

Si la empresa tuviera copias de seguridad locales, estas también se destruirían con el incendio, ya que estarían en el mismo edificio. Esto provocaría una pérdida casi total de los datos y la recuperación no sería viable.

c) Método 3-2-1

Si la empresa aplicara correctamente el método 3-2-1, tendría copias de seguridad disponibles en la nube o en otra ubicación externa. Esto permitiría una restauración completa de los datos, con un tiempo de recuperación aproximado de entre 4 y 24 horas.

d) Resumen de tiempos

Con solo RAID, el tiempo de recuperación sería infinito. Con copias locales, también sería infinito. En cambio, aplicando el método 3-2-1, la recuperación se podría realizar en un plazo de entre 4 y 24 horas.

e) Mini plan de recuperación

Primero se activa el plan de contingencia. A continuación, se accede a las copias de seguridad en la nube. Después, se restauran los servidores en una nueva ubicación. Seguidamente, se comprueba la integridad de los datos recuperados. Por último, se reanudan los servicios más importantes de la empresa.

3.5. Evaluación de dos escenarios

Empresa 1 – Trabajo con vídeo 4K

La mejor opción para esta empresa es utilizar **SSD NVMe con RAID 0**. Esta configuración ofrece la máxima velocidad de lectura y escritura, lo que es muy importante para trabajar con ficheros de vídeo muy grandes. En este caso, no es crítico perder algún dato, ya que el objetivo principal es el rendimiento. El uso de RAID 0 mejora mucho la velocidad, aunque no ofrezca tolerancia a fallos.

Empresa 2 – Datos financieros

Para esta empresa, la opción más adecuada es usar **RAID 10 junto con copias en la nube cifradas**. Esta solución ofrece alta disponibilidad y tolerancia a fallos, lo que es fundamental cuando se trabaja con datos sensibles. El cifrado es obligatorio para proteger la información personal y financiera. Además, esta configuración ayuda a cumplir con el RGPD y evita cualquier pérdida de datos, que en este caso sería inaceptable.