Una vez cumplido el tiempo de retención de los medios, se deben borrar los contenidos del mismo y disponer del medio para su reutilización.

No se podrá reutilizar un medio que aún no haya cumplido su plazo de retención. Por ejemplo, si una cinta magnética tiene un ciclo de reutilización cada 1 mes, el medio sólo podrá disponerse al superar dicho período.

Los medios extraíbles que no pueden ser reutilizados, como por ejemplo, por haber concluido su vida útil, por estar dañados o porque su formato no lo permite, deberán ser destruidos físicamente y luego desechados. El acto de destrucción deberá asegurar que no se pueda acceder al medio ni a la información contenida en el medio.

7.2.5. Información histórica, sin actualización o en desuso

Cuando exista información que por su condición o características no sufra modificaciones, como por ejemplo referida a periodos o ejercicios cerrados, sistemas en desuso, u otros, se podrá realizar un resguardo independiente a modo de Archivo histórico. Una vez resguardada la información original, podrá ser excluida del proceso de resguardo periódico, manteniéndose la información en su ubicación original.

Se deberá contemplar:

a) El Propietario de la Información autorizará formalmente la exclusión de la información histórica del proceso periódico de resguardo.
b) La información histórica, a pesar de su condición de inalterabilidad, deberá ser resguardada mínimamente una vez al año manteniéndose, al menos, las últimas 2 copias históricas que se realicen.
c) El medio de respaldo que contenga la información histórica deberá ser rotulado de forma tal que no se confunda con los resguardos periódicos.
d) Los medios de almacenamiento que contengan información Histórica deberán ser incluidos obligatoriamente en los procesos de prueba de restauración.
e) La preservación de archivos histórico eventualmente incluirá los recursos de software en las versiones que brinden accesibilidad a los datos objetos del resguardo.

7.2.6. Preservación de medios

Los dispositivos de almacenamiento se deterioran con el tiempo, son susceptibles a los fallos mecánicos, pueden sufrir las consecuencias de cualquier desastre (incendio, inundaciones, etc.), ser objeto de errores humanos en su manipulación (caídas, contacto con líquidos, etc.) o simplemente la obsolescencia del propio soporte. Por estos motivos es necesario llevar un control de la vida útil de los soportes físicos de resguardo y así evitar que cualquier posible deterioro afecte a la integridad de los datos en ellos contenidos.

Para garantizar la conservación e integridad de nuestros datos se deben seguir las siguientes pautas:

a) Comprobar la vida útil de los soportes que utilizamos para realizar las copias.
b) Realizar un mantenimiento de hardware y software periódico de los soportes de almacenamiento, ya que es tan importante prevenir los posibles fallos mecánicos como las posibles vulnerabilidades, infecciones e intrusiones que pueden derivar del software sin actualizar.
c) Asegurar que las condiciones de climatización del lugar donde se almacenan los dispositivos son adecuadas para conservar el tipo de soporte en el que guardamos la información.

Cuando la vida útil del soporte esté llegando a su fin, o los recursos informáticos se vuelvan obsoletos y sean remplazados por una nueva tecnología, o si las condiciones del soporte no son óptimas, se deberá copiar la información a un nuevo soporte para evitar la pérdida de los datos.

7.2.7. Respaldo Externo, fuera del sitio principal

Como parte del plan de recuperación ante desastre y para evitar la pérdida total de la información ante un incidente grave que afecte el sitio principal, como ser incendios, inundaciones, atentados, robo o destrucción, entre otros, se debe disponer de una copia de seguridad fuera del sitio principal, la cual debe ser actualizada periódicamente con un lapso no mayor a 3 meses.

Para que el respaldo externo sea efectivo, este debe contener todos los elementos necesarios para recuperarse del siniestro en el menor tiempo posible, suponiendo que el sitio principal ya no se encuentre disponible. Por dicho motivo, el respaldo externo debe incluir, además de los Datos a resguardar; instaladores, configuración, códigos fuentes, licencias, instructivos para la restauración, procedimientos y demás elementos necesarios que pudieran requerirse para reinstalar los ambientes y recuperarse del siniestro.

Al momento de seleccionar el sitio donde se alojará la copia de seguridad externa, se deberá tener en cuenta que el sitio reúna las mismas condiciones de seguridad, o superior, que el sitio principal y de ser posible, elegir una ubicación fuera del sitio principal, que se encuentre a una distancia suficiente para no verse afectado por el mismo incidente grave que afecta el sitio principal, por ejemplo un incendio en el edificio, una inundación, etc.

Los datos pueden ser transportados fuera de la ubicación principal utilizando medios de almacenamiento extraíbles, como cinta magnética o almacenamiento óptico, o por métodos electrónicos como copiado a centro de datos alternativos o copias en la nube. En todos los casos, es recomendable que los datos estén encriptados para asegurar que la información no pueda ser accedida por terceros.

8. Política de recuperación

1. El Propietario de la Información es el encargado de realizar la petición de recuperación al responsable del área informática ya sea ante la pérdida de datos total o parcial, u otros motivos.

2. La restauración de la información siempre se realizará en una ubicación diferente a la de la información original para poder ser verificada por el Propietario.
3. El responsable del área informática debe verificar que se restaure el backup solicitado, y
4. El Propietario de la Información o quien este designe, validará la integridad o contenido de la información y en caso de ser necesario, dará conformidad al proceso de recuperación.

8.1. Pruebas de recupero

Las pruebas de recupero deben realizarse periódicamente a intervalos no mayores a 6 (seis) meses. Su utilidad es la de verificar que el proceso de resguardo es correcto y que las restauraciones se pueden ejecutar con éxito.

Las pruebas de recupero siempre se deben realizar en una ubicación lógica diferente a la de la información original para no afectar los datos en producción.

En cada oportunidad que se realicen pruebas de recupero, se deberán incluir obligatoriamente los activos clasificados como críticos y de manera rotativa otros activos con menor criticidad, de manera de contemplarlos a todos en las sucesivas pruebas.

Si la prueba de recupero no es exitosa (el sistema no es recuperado, se perdieron datos, etc.) el responsable del área informática deberá verificar la metodología de resguardo y generar una nueva prueba, hasta que el resultado del recupero sea exitoso.

Cuando se realicen modificaciones en el proceso de resguardo, ya sea por cambios del proceso, inclusión de nueva información a resguardar u otro motivo, se realizarán nuevamente las pruebas de recupero del medio afectado.

El responsable del área informática deberá mantener un registro de las pruebas de recupero el cual debe contener, como mínimo:

- Medio de respaldo probado.
- Rótulo del resguardo recuperado.
- Breve descripción de la información recuperada.
- Resultado de las pruebas de recupero.
- Lugar y fecha donde se realizaron las pruebas de recupero.
- Personal interviniente en las pruebas de recupero.

La información recuperada debe validarse contra la información resguardada, para esto se pueden implementar Hash u otros mecanismos técnicos de control.

El Propietario de la Información, o quien este designe, debe validar la integridad o contenido de los datos e informar el resultado de la restauración al responsable informático.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Informe gráfico

Número:

Referencia: Política de Resguardo y Recuperación de la Información

---

El documento fue importado por el sistema GEDO con un total de 11 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.05.29 16:32:29 -03:00

Digitally signed by Gestion Documental Electronica
Date: 2023.05.29 16:32:29 -03:00