Copias de seguridad

una guía de aproximación para el empresario

protege tu empresa

ÍNDICE

1 INTRODUCCIÓN

1.1. Qué es una copia de seguridad

En el sentido más académico, una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.

Sin embargo, en el ámbito empresarial podríamos definir la copia de seguridad como la salvaguarda de nuestro negocio, una medida indispensable para garantizar su continuidad y conservar la confianza que nuestros clientes han depositado en nuestra organización. De lo contrario, podríamos proyectar una imagen negativa y generar desconfianza.

Toda empresa que proteja sus sistemas de información contará con un **Plan Director de Seguridad** [1], así como con un **Plan de Contingencia y Continuidad de Negocio** [2], en los que las copias de seguridad serán parte fundamental de ambas planificaciones.

El Plan Director de Seguridad marca las prioridades, los responsables y los recursos que se van a emplear para mejorar el nivel de seguridad y, por tanto, contemplará la **política de copias de seguridad** [3] que se debe adoptar en nuestra organización.

Por otro lado, el Plan de Contingencia y Continuidad de Negocio nos dará las pautas para responder de manera rápida y eficaz ante un incidente de seguridad, de forma que podamos restablecer la actividad de la empresa lo antes posible, intentando reducir así el impacto. Ante la posibilidad de enfrentarnos a pérdidas de información, nuestro Plan de Contingencia definirá la información que debe incluirse en las copias de seguridad, qué tipo de soporte se utilizará, con qué periodicidad y en qué instalaciones físicas se alojarán. Asimismo, se deberían definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información.

1

1.2. ¿Por qué hacer copias de seguridad?

Lo más probable es que manejes información importante y confidencial y dependes de ella para que tu negocio siga adelante. La pérdida de esta información supondría la pérdida de horas de trabajo y de proyectos que tendría graves consecuencias para la continuidad del negocio.

Hay que tener en cuenta que los soportes donde recogemos esa información suelen tener una vida útil limitada (averías, desgastes...) y están sujetos a diversos riesgos y/o amenazas (accidentes, ataques...). Por estos motivos tenemos que implementar las medidas para proteger el mayor activo que almacenamos en dichos soportes, la información, así que empecemos a hacer copias de seguridad.

2 ¿QUÉ INFORMACIÓN SE DEBE COPIAR?

2.1. Determinar la información que se copiará.

Para determinar cuál es la información de la que se realizará copia de seguridad, debemos realizar un inventario de activos de información[1] y una **clasificación** [4] de los mismos en base a su criticidad para el negocio. Los activos de información pueden estar en formato digital o en otros soportes (papel, película fotográfica, etc.). En formato digital pueden ser ficheros de todo tipo (texto, imagen, multimedia, bases de datos...), desde los programas y aplicaciones que los utilizan y gestionan hasta los equipos y sistemas que soportan estos servicios.

El objetivo de este procedimiento es tener un registro de todo el *software* y los datos imprescindibles para la organización, de manera que sirva para determinar la periodicidad de las copias y su contenido.

2.1.1 Criterios de clasificación de la información

Los criterios de clasificación que apliquemos a los activos de información deben estar relacionados con las medidas de seguridad que aplicaremos sobre nuestra información. Algunos de estos criterios podrían ser:

- **por el nivel de accesibilidad o confidencialidad:**
  - → Confidencial: accesible solo por la dirección o personal concreto.
  - → Interna: accesible solo al personal de la empresa.
  - → Pública: accesible públicamente.
- **por su utilidad o funcionalidad:**
  - → Información de clientes y proveedores.
  - → Información de compras y ventas.
  - → Información de personal y gestión interna.
  - → Información sobre pedidos y procesos de almacén.
- **por el impacto en caso de robo, borrado o pérdida:**
  - → Daño de imagen.
  - → Consecuencias legales.
  - → Consecuencias económicas.
  - → Paralización de la actividad.

1. Los activos de información son todos los recursos que traten información utilizados dentro de la organización y con valor para la empresa.

2

Como ejemplo orientativo, se muestra una clasificación de la información en función del nivel de accesibilidad o confidencialidad de la información:

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a la Dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. También datos de carácter personal, en particular los de categorías especiales.	Esta información debe marcarse adecuadamente. Se deben implementar todos los controles necesarios para limitar el acceso únicamente a aquellos empleados que necesiten conocer la información. En caso de sacarla de las instalaciones de la empresa en formato digital, debe cifrarse. Para los datos de carácter personal, se deben tener en cuenta la protección y garantías indicadas en la legislación sobre la materia.
Interna	Información propia de la empresa, accesible para todos sus empleados. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.	Esta información debe estar adecuadamente etiquetada y accesible para todo el personal. No debe difundirse a terceros, salvo autorización expresa de la dirección de la empresa.
Pública	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.	Esta información no está sujeta a ningún tipo de tratamiento especial.

2

"El ciclo de vida de la información determinará el momento en que dejará de ser útil y, por tanto, cuándo tenemos que eliminarla de manera segura."

Además, recuerda que al clasificar los activos de información debemos establecer su ciclo de vida, que dependerá de la vida útil del soporte y de la vigencia de su contenido. Si el soporte caduca antes que el contenido, tendremos que volcarlo a otro soporte para garantizar su conservación. El ciclo de vida de la información determinará el momento en que dejará de ser útil y, por tanto, cuándo tenemos que eliminarla de **manera segura** [5].

2.2. Periocidad y tipo de copias

Para determinar la frecuencia con la que debemos realizar copias de seguridad, será necesario realizar un análisis en el que se tengan en cuenta los siguientes factores:

- **el número de datos o archivos generados y/o modificados**;
- **el coste de almacenamiento** [6];
- **las obligaciones legales**, por ejemplo, el **Reglamento Europeo de Protección de Datos (RGPD)** [7] obliga a cualquier empresa que trate datos de carácter personal, a establecer procedimientos de actuación para la realización de copias de respaldo.

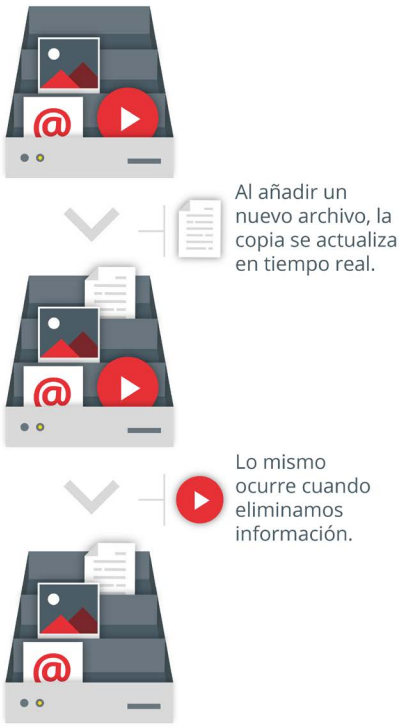
Teniendo en cuenta los elementos anteriormente citados, debemos elegir el **tipo de copia de seguridad** que nos ofrecen las aplicaciones para realizar respaldos, siendo las siguientes las más comunes:

2.2.1 Copia de seguridad en espejo o RAID 1

Una copia de seguridad en espejo, también conocida como RAID 1, crea una copia exacta de los datos en tiempo real. Es decir, mientras trabajas con la información creas una copia espejo en una ubicación alternativa.

Sus principales ventajas son las siguientes:

- **La copia se realiza en tiempo real.**
- **La recuperación de los datos es un proceso muy ágil.**
- **No se almacenan archivos antiguos o en desuso.**



Copia de seguridad en espejo

Al tratarse de una copia en espejo, si borramos un archivo accidentalmente también lo estaremos borrando de la copia de seguridad, por lo tanto, su mayor desventaja reside en la posible pérdida de archivos.

2.2.2 Copia de seguridad completa

Se trata del tipo de copia de seguridad más básica y probablemente la más realizada. Consiste, como su propio nombre indica, en hacer una copia de todos los datos de nuestro sistema en otro soporte. La ventaja principal de este tipo de copia es que proporciona una fácil restauración de los datos, ya que todos los datos han sido copiados.

Sin embargo, existen varios inconvenientes en este tipo de copias:

- Tienen una **mayor necesidad de espacio de almacenamiento** frente a los otros tipos de copias, puesto que se copian todos los ficheros de nuestro sistema cada vez que se realiza la copia de seguridad, lo que implica tener información redundante, ya que almacenaremos múltiples veces todos los ficheros, incluso los que no han sufrido ninguna modificación.
- **La ventana de copia de seguridad[2] es mayor** frente a otros tipos de copias.
- No es recomendable realizar una copia completa en horario laboral por **la carga que conlleva sobre el servidor y los sistemas**. Como consecuencia podría ralentizar los equipos o recursos que están siendo utilizados (ordenadores, acceso al servidor, etc.)
- **Coste elevado**, debido a que se necesita mucho espacio de almacenamiento.

"Un buen Plan de Contingencia y Continuidad de negocio debe incluir **copias de seguridad** completas cada cierto tiempo."

Un buen **Plan de Contingencia y Continuidad de negocio** [2] debe incluir copias de seguridad completas cada cierto tiempo. Por ejemplo, una vez a la semana o una vez al mes (dependiendo de las necesidades de almacenamiento, la cantidad de información generada o modificada y de la criticidad de esta), y siempre combinándolo con copias incrementales o diferenciales. Puedes consultar un ejemplo más concreto en el apartado 5.3 'Periodo de conservación'.

2. Ventana de copia de seguridad: el tiempo que tarda en finalizarse una copia de seguridad desde el inicio hasta el final.

2

"Una copia de seguridad incremental solo copia los datos que han variado desde la última copia de respaldo realizada, ya fuera incremental, diferencial o completa."

2.2.3 Copia de seguridad diferencial

Una copia de seguridad diferencial es similar a una copia incremental en la primera vez que se lleva a cabo, ya que se copiarán todos los datos que hayan cambiado desde el respaldo anterior. Sin embargo, cada vez que se vuelva a lanzar, no solo se copiarán los datos que se hayan modificado desde la última copia, si no todos los que se hayan modificado desde la última copia completa realizada. Esto significa que, con el tiempo, estos tipos de copia se van haciendo más grandes, hasta que se vuelve a realizar la copia completa.

» **Las principales ventajas son:**

→ No requieren tanto espacio de almacenamiento como una copia completa.

→ A la hora de recuperar un fichero, solo habrá que comprobar su existencia en dos copias de respaldo: la última copia diferencial realizada y la última copia completa realizada.

» **Entre sus desventajas podemos destacar:**

→ No es la solución más optimizada en cuanto a espacio. En este sentido la copia es considerable (sin ser tan alta como la de la copia completa).

→ La ventana de copia es considerable (sin ser tan alta como la de la copia completa).

2.2.4 Copia de seguridad incremental

Una copia de seguridad incremental **solo copia los datos que han variado desde la última copia de respaldo realizada**, ya fuera incremental, diferencial o completa. Las aplicaciones de *backup* registran la fecha y hora de una copia de seguridad, de manera que, cuando se realiza una copia incremental, dicha aplicación busca la fecha de la última copia y solo almacena los archivos que han sido modificados en el sistema desde esa fecha registrada hasta el momento actual.

Como este tipo de respaldo no almacena todos los ficheros, sino solo los ficheros modificados desde la anterior copia, las ventajas principales son:

2

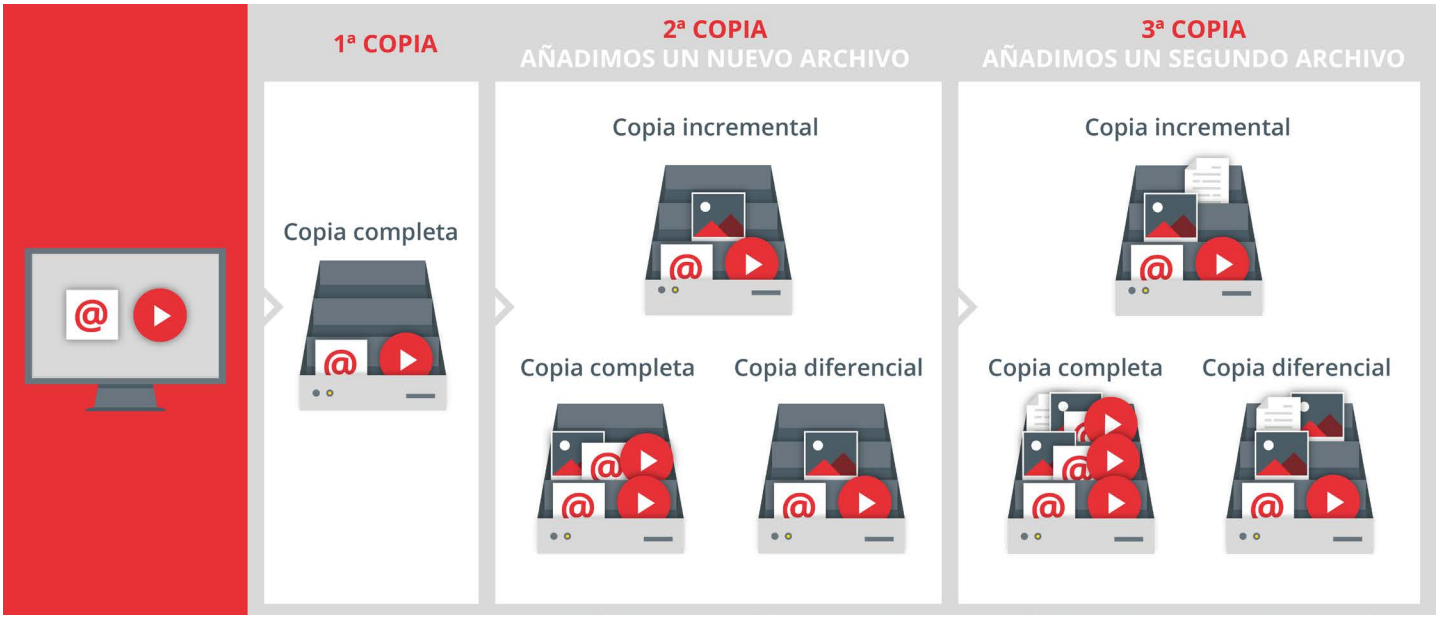
"Recuerda que siempre puedes optar por apoyarte en tu proveedor tecnológico para que te ayude con la gestión de las copias de seguridad y a determinar las medidas técnicas y organizativas necesarias que mejor se adapten a tu **organización**."

- **El espacio** necesario es mucho menor que el que requiere una copia completa.
- **El tiempo** de realización de la copia de seguridad es mucho más corto.

El inconveniente de este tipo de copias reside en la recuperación de los datos. Si, por ejemplo, queremos recuperar un directorio completo cuyos ficheros se han ido modificando poco a poco debemos recuperar los diferentes ficheros de las distintas copias incrementales, ralentizando así el proceso de recuperación.

Para evitar este gran inconveniente existen aplicaciones de copias de datos que permiten realizar copias por versiones de archivos, facilitando así su recuperación[3].

La siguiente imagen muestra las diferencias entre las distintas copias de seguridad:



Tipos de copias de seguridad

Recuerda que siempre puedes optar por apoyarte en tu proveedor tecnológico[4] para que te ayude con la gestión de las copias de seguridad y a determinar las medidas técnicas y organizativas necesarias que mejor se adapten a tu **organización** [3].

3.Consulta el punto 3. ¿Dónde almaceno mi copia de seguridad?, concretamente los dispositivos NAS.

4.Consulta el Catálogo de empresas y soluciones de seguridad para encontrar el proveedor adecuado

3 ¿DÓNDE ALMACENO MI COPIA DE SEGURIDAD?

El soporte escogido para realizar la copia de seguridad dependerá de la cantidad de información que necesitemos salvaguardar, del sistema de copia seleccionado y de la inversión que deseemos realizar. Estas tres variables van estrechamente unidas y deben estar en consonancia con nuestra política de copias de seguridad.

A continuación, se presentan los distintos dispositivos de almacenamiento que podemos tener en cuenta a la hora de guardar las copias de seguridad.

Cintas magnéticas DAT/DDS (*Digital Audio Tape/Digital Data Storage*) / LTO (*Linear Tape-Open*): la principal ventaja de este medio de almacenamiento es su reducido coste para almacenar grandes cantidades de datos por lo que, a pesar de surgir nuevas tecnologías para almacenar las copias de seguridad que proporcionan un almacenamiento y extracción de datos mucho más rápido, las cintas magnéticas siguen teniendo su público. Se han realizado estudios[5] que demuestran el auge de esta tecnología como medio de almacenamiento para las copias de seguridad por considerarse más fiables que los discos duros, poseer una vida útil superior a 30 años y un menor coste por terabyte.

Debido al impacto del ***ransomware*** [8], cada vez son más las empresas que se conciencian sobre la importancia de realizar copias de seguridad.

Discos duros (HDD y SSD): el almacenamiento de las copias de seguridad en discos externos presenta las siguientes ventajas:

- **Mayor facilidad de configuración** frente a las cintas magnéticas.
- **Pueden configurarse en RAID[6]**, de manera que permiten una mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad de almacenamiento.
- **Mejores tasas de rendimiento** que las cintas magnéticas.

5. https://www.wsj.com/articles/companies-look-to-an-old-technology-to-protect-against-new-threats-1505700180.

6. Un grupo/matriz redundante de discos independientes (también, RAID, del inglés *redundant array of independent disks*) hace referencia a un sistema de almacenamiento de datos que utiliza múltiples unidades (discos duros o SSD), entre las cuales se distribuyen o replican los datos.

3

"El almacenamiento en la nube se basa en salvaguardar nuestras copias de seguridad en servidores de terceros."

Si se trata de una pequeña empresa, las copias de seguridad basadas en discos duros pueden realizarse en **dispositivos NAS** (del inglés *Network Attached Storage*)[7]. Su coste varía en función del número y tipo de discos empleados, por lo que podemos elegir la solución que mejor se adapte a nuestra organización. La gestión de las copias de seguridad es mucho más sencilla en un dispositivo central de almacenamiento que en varios discos duros individuales y nos permite realizar copias de seguridad de los datos de cada equipo conectado a la red y de dispositivos móviles. Una de sus ventajas es que los principales fabricantes de NAS disponen de aplicaciones de copia de seguridad que se encargan de realizar copias por versiones de archivos, facilitándonos su recuperación si a causa de algún tipo de incidente hemos perdido nuestra información.

Para empresas de mayor tamaño existen otro tipo de soluciones profesionales[8], implantación de Planes de Seguridad y Contingencia y dispositivos de *backup* que ofrecen protección de datos, rápida recuperación en caso de pérdida de información e integración de aplicaciones empresariales (ERPs, gestores de bases de datos, etc.).

Su considerable coste sería su mayor inconveniente frente al uso de las cintas magnéticas, si bien el precio de estos dispositivos cada día es más competitivo.

La nube: el almacenamiento en la nube se basa en salvaguardar nuestras copias de seguridad en servidores de terceros. Por lo tanto, nuestra única preocupación será la de exigir las **garantías de seguridad pertinentes** [9] a la empresa que se encargue de facilitarnos dicho servicio. Las ventajas del almacenamiento en la nube son claras:

- Poseemos una **copia de seguridad fuera de la empresa**.
- Nos asegura la **disponibilidad de los datos** en cualquier momento y, por tanto, la continuidad de negocio.
- La copia está **protegida ante cualquier incidente** que pueda ocurrir dentro de la organización.

7. Un sistema NAS es un dispositivo de almacenamiento conectado a una red que permite almacenar y recuperar los datos en un punto centralizado para usuarios autorizados de la red y múltiples clientes.

8. Consulta el Catálogo de empresas y soluciones de seguridad para encontrar el proveedor adecuado

3

Si utilizas servicios *cloud* para almacenar, recuerda cifrar todas tus copias de seguridad. Aunque la copia de seguridad no contenga datos personales, cifrar los datos corporativos siempre es una buena práctica, ya que estamos protegiendo nuestros datos en caso de **fuga de información** [10].

En cuanto a las desventajas, cabe destacar:

- **La confidencialidad**, puesto que estamos enviando la información con la que trabajamos a un tercero. Por lo tanto, se deberán firmar Acuerdos de Nivel de Servicios (ANS) con el **proveedor** [11], que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias.
- **Dependencia de la conexión a Internet** a la hora de restaurar las copias de seguridad.
- Se necesita un **ancho de banda de subida elevado** para garantizar el envío de las copias en un tiempo adecuado.

"Una **buena práctica** que hemos de contemplar es revisar la seguridad que pedimos a nuestro proveedor de servicios en la nube y elegir aquellos que estén certificados."

Una buena práctica que hemos de contemplar es revisar la seguridad que pedimos a nuestro proveedor de servicios en la nube y elegir aquellos que estén certificados o los servicios de intermediarios de seguridad en la nube denominados **Agentes de Seguridad para el Acceso a la Nube**[9] (o CSAB38 *Cloud Security Access Brokers*).

Discos ópticos: la utilización de *blu-rays* como dispositivos de almacenamiento está ganando popularidad dentro de las empresas que no necesitan una gran capacidad de almacenamiento ni hacer copias de seguridad muy frecuentemente y con un presupuesto ajustado. Uno de sus mayores atractivos es la protección que ofrece ante posibles ataques de tipo *ransomware* dirigidos a las copias de seguridad, ya que los blu-rays no pueden ser modificados una vez hayan sido grabados.

Como desventaja cabe destacar su posible deterioro a medio/largo plazo, pudiendo imposibilitar la recuperación de la copia.

9. Lee el artículo de M. A. Mendoza en Welivesecurity de ESET Seguridad en la nube para empresas: ¿Qué son los CASB? https://www.welivesecurity.com/laes/2014/09/24/seguridad-nube-empresas-que-son-casb/

3

Soluciones mixtas

Las soluciones mixtas ofrecen una combinación de distintos soportes de copias que podemos valorar según las necesidades de nuestra organización. Entre estas soluciones podemos destacar:

» **D2D2T (*Disk to Disk to Tape*)**: solución disco a disco a cinta. Los datos se copian inicialmente en un sistema de almacenamiento en disco. Una vez las copias estén alojadas en el sistema de almacenamiento en disco, se copiarán de nuevo en un sistema de almacenamiento en cinta de forma periódica. Esta solución rebaja el coste de almacenamiento de las copias de seguridad, puesto que los discos pueden reutilizarse y las cintas tienen un menor coste.

Solución disco a disco a cinta

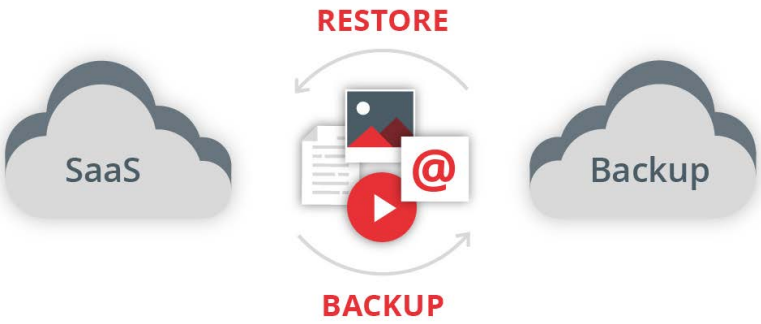
» **D2D2C (*Disk to Disk to Cloud*)**: solución disco a disco a nube, también conocida como copia de seguridad híbrida. A diferencia de la solución anterior, el almacenamiento en la nube ofrece la ventaja de que la copia de seguridad se encuentra fuera de las instalaciones de nuestra empresa. De la misma manera que en el concepto anterior, las copias se guardan primero en el sistema de almacenamiento en disco y posteriormente se replica en la nube.

Solución disco a disco a nube

"Las soluciones mixtas ofrecen una combinación de distintos soportes de copias que podemos valorar según las necesidades de nuestra organización."

3

C2C (*Cloud to Cloud*): solución nube a nube. En el mundo empresarial cada vez es más común el uso de aplicaciones SaaS (*Software as a Service*)[10] y, por lo tanto, la copia de seguridad nube a nube. Este tipo de aplicaciones no nos proporciona una garantía total de recuperación de datos en caso de pérdida, por lo que se hace necesario utilizar un respaldo adicional. Suele ser una práctica habitual que los propios proveedores de estas aplicaciones ofrezcan además su propio servicio de copia nube a nube.



Solución nube a nube

10.*Software as a Service*, SaaS, es un modelo de distribución de *software* donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación (TIC), a los que se accede vía Internet desde un cliente.

4 LA ESTRATEGIA 3-2-1 DE LAS COPIAS DE SEGURIDAD

Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia 3-2-1 que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable. Sus **claves de actuación** son las siguientes [12]:

- **3**: Mantener 3 copias de cualquier fichero importante: el archivo original y 2 *backups*.
- **2**: Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos. Si tuviéramos las dos copias en el mismo tipo de soporte, ambos pueden verse afectados por el mismo fallo de funcionamiento y por tanto poner en peligro las dos copias al mismo tiempo.
- **1**: Almacenar 1 copia de seguridad fuera de nuestra empresa, lo que también se conoce como *backup offsite*. La copia de seguridad en la nube es una clara opción de este tipo de copia.

Estrategia 3-2-1 de copias de seguridad

Imaginad que tenemos un fichero llamado «listadoproveedores.ots» al que queremos aplicar esta estrategia de copias de seguridad. Para ello debemos tener **3** copias de ese fichero. A la hora de cumplir los requisitos expuestos anteriormente este sería un ejemplo:

- Guardamos el archivo original en nuestro equipo.
- Almacenamos las dos copias en un disco duro externo y en un servicio de almacenamiento en la nube respectivamente. Ya tenemos nuestras copias en **2** soportes diferentes.
- Además, el almacenamiento en la nube cumpliría la premisa de *backup offsite* (**1** copia fuera del lugar de trabajo).

5 PROTECCIÓN DE LAS COPIAS

5.1. Ubicación de las copias de seguridad

Para garantizar la salvaguarda de las copias de seguridad, es necesario buscar un lugar adecuado para guardar las copias que cumpla con los siguientes criterios:

- contar con al menos una **copia fuera de la organización**;
- valorar la contratación de **servicios de guarda y custodia** si se considera necesario por motivos de **seguridad física** [13].

5.2. Control de soportes

Los dispositivos de almacenamiento se deterioran con el tiempo, son susceptibles a los fallos mecánicos, pueden sufrir las consecuencias de cualquier desastre (incendio, inundaciones...), ser objeto de errores humanos en su manipulación (caídas, contacto con el agua...) o simplemente la obsolescencia[11] del propio **soporte** [14]. Por estos motivos es necesario llevar un control de la vida útil de los soportes físicos de copia y así evitar que cualquier posible deterioro afecte a la integridad de los datos. Como ya se explicó en la estrategia 3-2-1, una buena práctica para proteger adecuadamente la información es almacenarla en dos tipos de soportes diferentes, así como en una ubicación fuera de las instalaciones de la empresa, evitando así que, en caso de que ocurra algún incidente en la organización, todas las copias de seguridad se vean afectadas y por lo tanto no sea posible llevar a cabo la recuperación, fallando así nuestro Plan de Contingencia y Continuidad de negocio.

Además, para garantizar la conservación e integridad de nuestros datos debemos seguir las siguientes pautas:

- Comprobar la **vida útil** de los soportes que utilizamos para realizar las copias.
- 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.
- Asegurar que las **condiciones de climatización del lugar** donde se almacenan son las adecuadas para conservar el tipo de soporte en el que guardamos la información.

11. La obsolescencia es la caída en desuso de las máquinas, equipos y tecnologías motivada no por un mal funcionamiento del estos, sino por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado.

5

5.3. Periodo de conservación

El periodo de conservación de las copias de seguridad variará dependiendo de las necesidades de cada organización, así como de los requerimientos legales a los que nuestra empresa deba estar sujeta. Debemos decidir cuánto tiempo mantener las copias en función de las siguientes consideraciones:

- **La información almacenada sigue vigente o es de utilidad** para nuestro negocio. En caso contrario debemos proceder a la eliminación de la información o a un borrado seguro del soporte. Recuerda que la ley define el periodo de conservación de la documentación contable de la empresa y de los datos personales hasta que finalice la prestación del servicio por el cual se hubieran **recabado** [15].
- **La vida útil del soporte** en el que se realizan las copias.
- **La necesidad de conservar varias copias anteriores a la última realizada**, como se muestra en el ejemplo del punto 5.3.1.

5.3.1 Modelo de copias de seguridad realizadas y su tiempo de conservación

Dependiendo del tipo de organización (tamaño, actividad, dependencia de la tecnología) variará la frecuencia de las copias de seguridad, así como la necesidad de conservación de estas.

A modo orientativo, esta sería una buena práctica a la hora de realizar y conservar copias de seguridad.

- **Copias incrementales diarias.**
- **Copias totales una vez a la semana.**
- **Conservación de las copias totales un mes.**
- **Almacenamiento de la última copia del mes durante un año.**

Es decir, en un mes se realizarían copias incrementales diariamente y 4 copias totales semanales. Cada copia total se conservará durante un mes y la última copia total de cada mes durante un año.

Tiempo de conservación de las copias de seguridad

5

5.4. Cifrado de las copias de seguridad

Para garantizar la confidencialidad e integridad de la información sensible cuando está almacenada, utilizaremos herramientas de cifrado que protejan nuestros datos, haciéndolos ilegibles por aquellos que no dispongan de la clave de cifrado.

Cifrando la información confidencial y la almacenada en copias de seguridad protegemos los datos en caso de robo de información o accesos no autorizados, reduce el riesgo de **sanciones y podría evitar**[12] [16] que tengamos que informar a los usuarios en caso de brecha de seguridad. Además, se cumplirá con el deber de salvaguarda que exige el **Reglamento General de Protección de datos** [17].

"Cifrando la **información confidencial** y la almacenada en copias de seguridad protegemos los datos en caso de robo de información o accesos no autorizados."

5.5. Restauración de las copias de seguridad

Las copias de seguridad son uno de los elementos esenciales que garantizan la continuidad de nuestro negocio y uno de los pilares principales del Plan de Contingencia por lo que, del mismo modo que comprobamos que nuestros dispositivos y aplicaciones funcionen correctamente, si no probamos que las copias de seguridad pueden restaurarse correctamente no garantizaremos que la información se pueda recuperar. No debemos asumir que por haber realizado el proceso de copia está todo hecho, por lo que debemos programar periódicamente pruebas de restauración de las copias para asegurar que el día que no sea una simulación se conocen todos los procesos y funcionan correctamente.

Ya hemos mencionado que, tanto los sistemas de copia como los soportes pueden fallar y es posible que llegado el momento en que sea necesario restaurar una copia, descubramos que no es posible cuando ya apenas tengamos tiempo de resolver la situación.

12. "Según el artículo 33 del RGPD, en caso de brecha de la seguridad que afecte a los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas."

5

Para minimizar el tiempo necesario de recuperación de los datos en caso de necesitar una restauración y así garantizar la continuidad de negocio, se han de elaborar y aplicar procedimientos que describan cómo hacer las copias y cómo restaurarlas. Esto nos permitirá, ante una contingencia real o ausencia del personal habitual, disponer de una guía que nos indique qué pasos debemos seguir para ejecutar la acción de generación o restauración de la copia con éxito.

Estos procedimientos deben revisarse al menos anualmente y siempre que haya un cambio importante en el inventario de activos de información. Además, hay que fijar una periodicidad para realizar pruebas de restauración para garantizar que la información respaldada puede ser recuperada en caso de desastre.

"hay que **fijar una periodicidad** para realizar pruebas de restauración para garantizar que la información respaldada puede ser recuperada en caso de desastre."

En resumen, el **objetivo final** de la realización de copias de seguridad es, además de poder restaurarlas en caso de que ocurra cualquier incidente que ocasione la pérdida de datos, mantener la continuidad de nuestro negocio en caso de desastre. Ante esta hipotética pero factible situación, a la hora de definir nuestra política de copias de seguridad, debemos tener en cuenta los siguientes conceptos:

Tiempo de recuperación o RTO (*Recovery Time Objective*)

Es el tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio (por ejemplo, debido a pérdida de datos) sin afectar a la continuidad de negocio.
El RTO de los recursos debe ser estimado por el personal técnico teniendo en cuenta las dependencias entre las distintas infraestructuras tecnológicas.

Tiempo máximo tolerable de caída o MTD (*Maximum Tolerable Downtime*)

Tiempo máximo tolerable de caída, que nos determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en la continuidad de negocio.

5

"El análisis de impacto en el negocio nos ayudará a identificar las necesidades del negocio en términos de recuperación."

Por ejemplo, si determinamos que el tiempo máximo tolerable de caída (MTD) de nuestro proceso de contabilidad son 24 horas y su RTO 8 horas:

→ Tardaremos 8 horas en volver a poner en marcha el proceso de contabilidad. en caso de desastre.

→ De no conseguir recuperar este proceso en 24 horas, puede verse afectada la continuidad de negocio.

Niveles mínimos de recuperación de servicio o ROL (*Revised Operating Level*)

Este es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo.
Aunque no siempre es posible determinar este valor, si nuestro proceso se basa por ejemplo en la atención de clientes a través de llamadas y online, podemos establecer un ROL en el 80%, tras lo cual consideraremos que el proceso está recuperado (lo que no implica que dejemos de aplicar las medidas de recuperación hasta el 100% para garantizar que el servicio vuelve a ser óptimo).

Grado de dependencia de la actualidad de los datos o RPO (*Recovery Point Objective*)

Es el periodo de tiempo máximo en el que la empresa asume la pérdida de datos. Si, por ejemplo, se determina que este periodo de tiempo es de 8 horas, se deben realizar copias de seguridad cada menos tiempo para poder recuperar la información antes de agotar dicho periodo.

Por ejemplo, si se ha determinado que nuestro proceso de contabilidad es muy crítico, pero puede utilizar datos históricos del mes pasado, su RTO será alto pero su RPO puede ser muy bajo.

Realizar un análisis de impacto en el negocio (también conocido como BIA, por sus siglas en inglés ***Business Impact Analysis***) [18] nos ayudará a identificar las necesidades del negocio en términos de recuperación (aquellas que consideramos indispensables para garantizar el funcionamiento de la organización).

5

5.6. Control de copias de seguridad

Debemos etiquetar e identificar los soportes dónde se realizan las copias de seguridad, de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado algún respaldo. Así, en el caso de tener que recuperar una información concreta, agilizaremos el proceso al poder consultar fácilmente en qué soporte se ha almacenado.

Por lo general, las aplicaciones que usemos para realizar las copias de seguridad nos proporcionarán la información necesaria (identificador de soporte, tipo de copia, fecha, etc.) que necesitamos para registrar las copias de seguridad realizadas.

A modo de ejemplo se presenta un posible diseño de una hoja de registro que deberá incluir los siguientes campos:

- **Identificador de soporte**: código que identifica el soporte en el que se ha realizado la copia.
- **Tipo de copia**: se indicará si es una copia total, incremental, etc.
- **Fecha y hora**: cuándo se llevó a cabo la copia.
- **Lugar de almacenamiento**: ubicación física donde se encuentra la copia de seguridad.
- **Personal a cargo de la copia**: responsables de la realización y conservación de la copia durante el tiempo que se haya establecido.

REGISTRO DE COPIAS DE SEGURIDAD	
Identificador de soporte	
Tipo de copia	
Fecha y hora	
Lugar de alamacenamiento	
Personal a cargo de la copia	

Registro de copias de seguridad

5

5.7. Borrado seguro y gestión de soportes

Cuando llega la hora de desechar los soportes que han sido utilizados para realizar copias de seguridad, debemos asegurarnos de destruirlos de forma segura.

Es muy importante cerciorarse de que esa información nunca volverá a ser accesible para evitar posibles accesos malintencionados, ya que estos datos pueden ser confidenciales y, por tanto, de gran interés para los ciberdelincuentes. Si la información llega a manos de terceros podría utilizarse de forma perjudicial para la empresa, llegando a tener incluso **implicaciones legales** [17].

Por estos motivos, si vamos a subcontratar la destrucción de nuestra información y soportes, debemos elegir la destrucción certificada[13] si se trata de datos personales o confidenciales y, en el caso de que nos viéramos obligados a ello, por un contrato o acuerdo con otra empresa. Esta opción nos asegura la destrucción de la información con las máximas garantías de seguridad y confidencialidad, desde la recogida del material documental hasta su destrucción física y eliminación final. Después de llevar a cabo la destrucción, la empresa emite un certificado que garantiza la validez de todo el proceso.

13. Consulta el Catálogo de empresas y soluciones de seguridad para encontrar el proveedor adecuado

5

A la hora de elegir el mejor método para eliminar la información, tendremos en cuenta las siguientes opciones:

» **En soportes no electrónicos y soportes magnéticos:**

→ Para eliminar la informaciónen este tipo de soportes (documentos impresos, CD, DVD, cintas magnéticas, radiografías, etc.) debemos utilizar la opción de triturado.

» **Para la reutilización de soportes electrónicos:**

→ Si queremos reutilizar un soporte que ya contiene datos, debemos utilizar la opción de sobreescritura para garantizar un borrado total de la información. Este metodo se puede utilizar en todos los dispositivos regrabables (discos duros, *pendrives* o pinchos USB, etc.) siempre que el dispositivo no esté dañado.

» **Antes de deshacernos de los soportes electrónicos:**

→ Cuando queremos desechar algún soporte de almacenamiento porque ya no funcione correctamente o porque se haya quedado obsoleto, debemos utilizar los métodos de desmagnetización o **destrucción física [5]**. Cualquiera de estos dos métodos imposibilita la reutilización del dispositivo garantizando que la información no pueda ser recuperada.

6 COPIAS DE SEGURIDAD EN DISPOSITIVOS MÓVILES

Los dispositivos móviles se han convertido en un elemento de uso indispensable en la vida profesional. Se guardan contactos del entorno empresarial, se envían y reciben correos a través de la cuenta corporativa y se manejan documentos y un sinfín de información corporativa imprescindible para llevar a cabo nuestro trabajo diario. Por estos motivos, debemos asumir que la protección de la información en los dispositivos móviles es tan importante como la protección en los equipos de trabajo.

A pesar de ser herramientas tan importantes de trabajo suelen ser los «grandes olvidados» a la hora de programar las copias de seguridad. Tanto si los dispositivos son propiedad de la empresa como si pertenecen al propio empleado (lo que se conoce como ***Bring Your Own Device*** **"BYOD"** [19] o, lo que es lo mismo, tráete tu propio dispositivo), deben de formar parte del Plan de Contingencia y Continuidad del negocio, al igual que el resto de los dispositivos.

Existen soluciones como las de Gestión de Contenidos Móviles o MCM (del inglés *Mobile Content Management*), que nos facilitan la tarea de salvaguardar la información de los dispositivos móviles. Son sistemas que garantizan la seguridad de los datos corporativos mediante funcionalidades de protección de la información, como el cifrado de datos, y previenen la fuga de datos corporativos controlando:

- **la sincronización de estos dispositivos con otros equipos o dispositivos externos de almacenamiento** como USB o discos duros externos;
- **la sincronización con servicios de almacenamiento en la nube**;
- **los ficheros adjuntos de los correos electrónicos**;
- **los datos gestionados por las apps de los dispositivos**.

La realización de copias de seguridad no nos protege de los ataques a los que podamos estar expuestos, pero nos garantiza que podremos recuperar la información importante si el dispositivo se vuelve inaccesible: pérdida o robo del terminal, fallo en el funcionamiento del dispositivo, borrado accidental, etc.

6

"Si las copias deben incluir **datos personales** de los usuarios propietarios de los dispositivos, deben aplicarse las medidas necesarias para proteger la privacidad de estos datos."

Las medidas a tener en cuenta a la hora de realizar copias de seguridad en dispositivos móviles son las siguientes:

- **Las copias realizadas se deben almacenar fuera del dispositivo.** Dos posibles alternativas son los servidores de nuestra empresa y la nube, siempre teniendo en cuenta las garantías de seguridad que debemos exigir cuando se trata de la nube.
- **En el caso en que los dispositivos sean propiedad de los empleados**, las copias generadas serán almacenadas en lugares gestionados por la empresa y controlados por el personal técnico, en lugar de utilizar dispositivos personales de los empleados o en sistemas que estén fuera del control del personal técnico. Si las copias deben incluir datos personales de los usuarios propietarios de los dispositivos, deben aplicarse las medidas necesarias para proteger la privacidad de estos datos personales recogidas por el **RGPD** [17]. Cuando el empleado utiliza su terminal para realizar su trabajo, deberá garantizar la seguridad en dicho dispositivo aunque esto implique restringir ciertas funcionalidades.

6

- **Se recomienda que las copias se hagan periódicamente y de manera automática**, por ejemplo, cada noche si la jornada laboral transcurre durante el día. Si trabajamos con información crítica[14], es interesante conocer que algunos servicios de almacenamiento en la nube disponen de la opción de realizar una copia de seguridad cada vez que se detectan cambios en los archivos.
- **El número y la periodicidad de las copias dependerán de las necesidades propias de cada organización**. Se recomienda adecuarlas en función del tipo de dispositivos, el volumen y tipo de información que se gestiona y su frecuencia de modificación.
- **Debe ser posible lanzar procesos manuales de copia** de seguridad para garantizar que pueden realizarse en caso de que el sistema automático no funcione correctamente.
- Como ya apuntamos anteriormente, es tan importante hacer copias de seguridad de la información como **comprobar que se han realizado con éxito y que se pueden restaurar**. De nada nos servirá tener almacenada nuestra información en copias de seguridad si no nos aseguramos de que se puede restaurar la información a su estado y ubicación original.
- **Comprobar periódicamente que el soporte sobre el que se hacen las copias está en buen estado** y programar revisiones de mantenimiento.

14. Podemos definir la información crítica en una empresa como aquella que está sujeta a la ley, la que, si nos faltara, por su confidencialidad o si se corrompiera, paralizaría nuestra actividad y nos acarrearía pérdidas de imagen o económicas.

7 RESUMEN

Después de leer esta guía seguro que tienes más claro por qué es tan necesario realizar copias de seguridad en la empresa. A modo de resumen, consulta este apartado siempre que necesites recordar los pasos más importantes a la hora de realizar copias de seguridad.

» **¿De qué se debe hacer copias de seguridad?**

→ La información crítica corporativa, la obligatoria por ley y por contratos con terceros.
→ Toda la información necesaria para garantizar la continuidad de negocio.

» **¿Cada cuánto tiempo es necesario realizarlas?**

→ Será necesario buscar la relación óptima entre la variación de los datos y el coste de almacenamiento.

» **¿Qué tipo de copia puedo elegir?**

→ Completa: todos los datos de nuestro sistema se copian en otro soporte.
→ Incremental: se copian los datos que han variado desde la última copia de respaldo realizada.
→ Diferencial: se copiará todo lo que se haya modificado desde la última copia completa realizada.
→ En espejo: se crea una copia exacta de los datos en tiempo real.

» **¿Cuánto tiempo deben conservarse las copias?**

→ Define la vigencia en función de la necesidad de reemplazo por otras nuevas.
→ Contempla los aspectos legales aplicables en tu organización.
→ Valora la duración del soporte.
→ Conserva más de una copia de situaciones anteriores y no solo la ultima.

» **Comprobar la validez de las copias**

→ Comprueba periodicamente que las copias pueden restaurarse.

» **Cifrado de la información**

→ Cifra la información crítica, la que almacenes en la nube o en proveedores externos y la obligatoria por ley.

» **Elección de soportes**

→ Valora su coste, fiabilidad, tasa de transferencia y capacidad.
→ Utiliza siempre soportes en buen estado.
→ Registra su ubicación y vida útil, así como quién tiene acceso a los mismos.
→ Bórralos o destrúyelos de forma segura al final de su vida útil.

7

» ¿Dónde almaceno las copias?

→ Al menos una copia fuera de la organización.
→ No utilices dependecias personales.
→ Valora si es necesario la guarda y custodia.

» Consideraciones para las copias en la nube

→ Cifra la información antes de hacer la copia.
→ Firma acuerdos de Nivel de Servicio (ANS).
→ Considera el ancho de banda para subir y bajar las copias.

» Documentación del proceso

→ Documenta todo el proceso de realización y restauración de copias.

8 REFERENCIAS

[1] Plan Director de Seguridad

[2] Plan de Contingencia y Continuidad de Negocio

[3] Políticas de seguridad para la pyme – Copias de seguridad

[4] Políticas de seguridad para la pyme – Clasificación de la información

[5] Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes

[6] Políticas de seguridad para la pyme – Almacenamiento en la red corporativa

[7] Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario

[8] *Ransomware*: una guía de aproximación para el empresario

[9] Contratación de servicios

[10] Cómo gestionar una fuga de información: una guía de aproximación al empresario

[11] Políticas de seguridad para la pyme – Relación con proveedores

[12] US-CERT, *Data Backup Options*

[13] Catálogo de empresas y soluciones de ciberseguridad

[14] Borrado seguro de la información: una aproximación para el empresario

8 REFERENCIAS

[15] AEPD, Directrices para la elaboración de contratos entre responsables y encargados del tratamiento

[16] AEPD, Guía para la gestión y notificación de brechas de seguridad

[17] RGPD para pymes

[18] Pasos a seguir para realizar un análisis de impacto en nuestro negocio

[19] Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario

[20] Wikipedia, Definición de RAID

[21] Wikipedia, Definición de obsolescencia

[22] Wikipedia, Definición de SaaS

protege
tuempresa