¿Qué es una copia de seguridad?

¿Por qué debo hacerlas?

¿Qué información debo copiar?

Clasificación de la información

¿Con qué frecuencia debo hacerlas?

¿Dónde almaceno las copias de seguridad?

Cintas magnéticas

Discos duros

Nube

Ventajas

Desventajas

Estrategia 3-2-1

Protección de las copias

Control de soportes

Periodo de conservación

Cifrado

Restauración

Borrado seguro y gestión de soportes

Las copias de seguridad son de vital importancia. Permiten tener un respaldo extra de cualquier información en caso de que sufrieran algún incidente que hiciese desaparecer los datos originales.

Se puede dar la circunstancia de que los archivos se borren por un virus o cualquier otra causa.

Las copias de seguridad serán muy útiles en estas situaciones porque se podrán restaurar para recuperar la información original. Todo con el objetivo de que puedas volver a tener acceso a esos datos perdidos.

Por eso aquí tienes toda la información sobre las copias de seguridad.

### ¿QUÉ ES UNA COPIA DE SEGURIDAD?

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.

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.

### ¿Por qué debo hacerlas?

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 empieza a hacer copias de seguridad.

### ¿Qué información debo copiar?

Para determinar cuál es la información de la que se realizará copia de seguridad, debemos realizar un inventario de activos de información y una clasificación de los mismos en base a su criticidad para el negocio.

La información puede 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.

### Clasificación de la información

Los criterios de clasificación aplicados 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

Datos de clientes y proveedores.

Información de compras y ventas.

Datos de personal y gestión interna.

Información sobre pedidos y procesos de almacén.

Por el impacto en caso de robo, borrado o pérdida

Daño a la imagen

Consecuencias legales

Consecuencias económicas

Paralización de la actividad

Además, es importante que al clasificar los activos de información determines su ciclo de vida, que dependerá de la vida útil del soporte y de la vigencia de su contenido.

### ¿Con qué frecuencia debo hacerlas?

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:

Número de datos o archivos generados y/o modificados

Coste de almacenamiento

Obligaciones legales. Por ejemplo, el Reglamento Europeo de Protección de Datos (RGPD) obliga a cualquier empresa que trate datos de carácter personal, a establecer procedimientos de actuación para la realización de copias de respaldo.

### ¿DÓNDE ALMACENO LAS COPIAS DE SEGURIDAD?

El soporte escogido para realizar la copia de seguridad dependerá de:

cantidad de información que necesitemos salvaguardar,

sistema de copia seleccionado e

inversión que deseemos realizar.

Los principales dispositivos de almacenamiento de información son:

### Cintas magnéticas

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.

### Discos duros

Entre sus ventajas están: mayor facilidad de configuración frente a las cintas magnéticas, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad de almacenamiento.

### 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 a la empresa que nos facilite ese servicio.

### Ventajas

Entre las ventajas de almacenar nuestras copias de seguridad en la nube cabe destacar:

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.

Si utilizas servicios cloud para almacenar, recuerda cifrar todas tus copias de seguridad. Así protegerás tus datos en caso de fuga de información.

### Desventajas

Entre las principales desventajas están:

La confidencialidad, puesto que estamos enviando la información con la que trabajamos a un tercero. Debemos firmar Acuerdos de nivel de servicio con el proveedor para garantizar 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.

### Estrategia 3-2-1

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.

Consiste en:

Mantener 3 copias de cualquier fichero importante: el archivo original y 2 backups.

Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos. En caso de tener 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.

Almacenar 1 copia de seguridad fuera de nuestra empresa. La copia de seguridad en la nube es una clara opción de este tipo de copia.

### PROTECCIÓN DE LAS COPIAS

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.

Control de soportes

Con el paso del tiempo, los dispositivos de almacenamiento:

se deterioran,

son susceptibles a los fallos mecánicos,

pueden sufrir las consecuencias de cualquier desastre (incendio, inundaciones…),

son objeto de errores humanos en su manipulación (caídas, contacto con el agua…) o

se vuelven obsolescentes.

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.

### 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 de seguridad atendiendo a:

Si la información almacenada sigue vigente o es de utilidad para nuestro negocio.

Vida útil del soporte en el que se realizan las copias.

Necesidad de conservar varias copias anteriores a la última realizada.

Cifrado

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 y reduce el riesgo de sanciones.

Además, se cumplirá con el deber de salvaguarda que exige el RGPD.

### Restauración

Si no probamos que las copias de seguridad pueden restaurarse correctamente no garantizaremos que la información se pueda recuperar. 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.

Debemos elaborar 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.

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.

### Borrado seguro y gestión de soportes

A la hora de desechar los soportes 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.

Si vamos a subcontratar la destrucción de nuestra información y soportes, debemos elegir la destrucción certificada si se trata de datos personales o confidenciales.

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

Soportes no electrónicos y soportes magnéticos: para eliminar la información en estos soportes debemos usar la opción de triturado.

Reutilizar soportes electrónicos: debemos utilizar la opción de sobreescritura para garantizar un borrado total de la información.

Antes de deshacernos de los soportes electrónicos debemos utilizar los métodos de desmagnetización o destrucción física.