PROTECCIÓN DE LA INFORMACIÓN

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

ÍNDICE

1- INTRODUCCIÓN 03
2- DESCRIPCIÓN DEL PROBLEMA 04
3- DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN 06
4- SELECCIÓN DE SALVAGUARDAS 08
4.1. IMPORTANCIA DE LA INFORMACIÓN PARA LA EMPRESA 09
4.2. PASOS PREVIOS A LA SELECCIÓN DE SALVAGUARDAS 11
4.3. NATURALEZA DE LOS CONTROLES 13
4.4. RESUMEN DE CRITERIOS DE SELECCIÓN 14
5- SALVAGUARDAS BÁSICAS 15
5.1. CONTROL DE ACCESO A LA INFORMACIÓN 16
5.2. COPIAS DE SEGURIDAD 20
5.3. CIFRADO DE INFORMACIÓN 25
5.4. DESECHADO Y REUTILIZACIÓN DE SOPORTES Y EQUIPOS 26
5.5. ALMACENAMIENTO EN LA NUBE 28
5.6. CONFIDENCIALIDAD EN LA CONTRATACIÓN DE SERVICIOS 30
6- REFERENCIAS 31

ÍNDICE

ÍNDICE DE FIGURAS

Ilustración 1: Dimensiones de la seguridad de la información **06**

Ilustración 2: Pasos previos a la selección de medidas para proteger la información **12**

Ilustración 3: Criterios selección salvaguardas **14**

Ilustración 4: Soportes para realizar copias de seguridad..... **20**

Ilustración 5: Tipos de copias de seguridad **23**

ÍNDICE DE TABLAS

Tablas 1: Errores más comunes en el tratamiento de la información en la empresa **05**

Tablas 2: Ejemplo clasificación información..... **11**

Tablas 3: Ejemplo de perfiles y permisos sobre los activos de información..... **17**

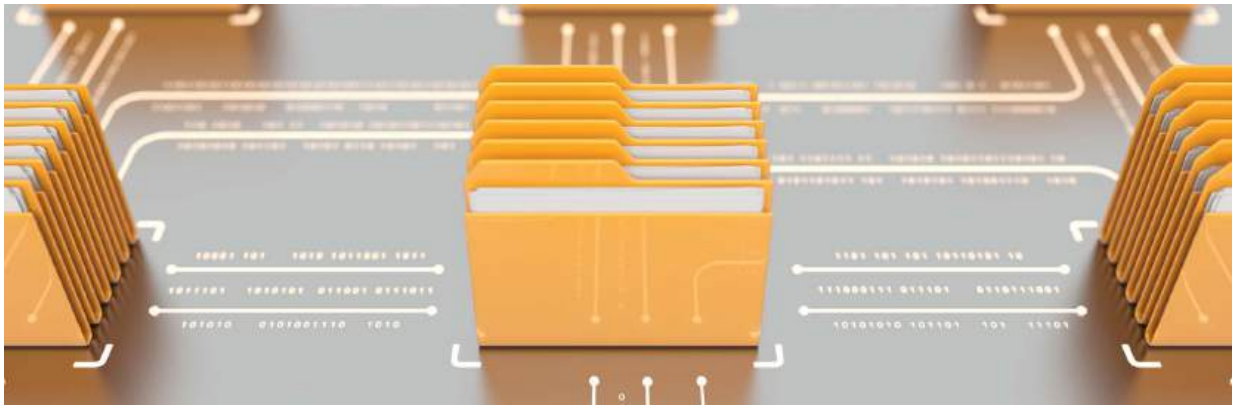
1. INTRODUCCIÓN

En el mundo empresarial, hay una tendencia generalizada a considerar como activos de la empresa únicamente los bienes tangibles: mobiliario, maquinaria, servidores, etc. Sin embargo, no debemos olvidar que existen bienes intangibles como la cartera de clientes, las tarifas, el conocimiento comercial, la propiedad intelectual o la reputación. Todos estos elementos forman parte de **la información de nuestra empresa y constituyen uno de los activos más importantes de nuestra organización.**

Existen empresas que basan su negocio en el tratamiento de información, como las que se dedican a la publicidad, prensa, radio, TV, contenidos multimedia, operadoras, etc. Pero no debemos pensar que son las únicas que han de preocuparse por la seguridad de la información. Es un error común pensar que en el ámbito de una pequeña empresa no es necesaria la protección de la información.

Pensemos, por ejemplo, en las tarifas o las ofertas que presentamos a nuestros clientes, las cuales nos permiten posicionarnos en el mercado o frente a la competencia, o en nuestros planes estratégicos para el crecimiento de nuestro negocio. Recapacitemos sobre las consecuencias que tendría la pérdida de la contabilidad de la organización, la cartera de clientes, la información confidencial que tenemos sobre nuestros clientes como sus cuentas bancarias o las propiedades intelectuales de nuestra empresa.

Todos estos ejemplos forman parte de la información de nuestra empresa, lo que la convierte en un activo vital que debe protegerse adecuadamente. Esto es lo que conocemos como **seguridad de la información.**



2. DESCRIPCIÓN DEL PROBLEMA

Gracias al uso de la tecnología, el procesamiento y almacenamiento de grandes volúmenes de datos se ha vuelto muy sencillo. En una memoria USB se podría almacenar, sin autorización para ello, una gran cantidad de información confidencial de una empresa de tamaño mediano e incluso a través de correo electrónico se podría enviar información confidencial de la empresa como la base de datos de clientes, con fines distintos a los permitidos.

En la empresa estos son los principales errores en el tratamiento de la información y la forma de evitarlos:

ERRORES	CÓMO EVITARLOS
Información importante de la que no se realiza copia de seguridad.	Para evitar cometer este error tendremos que asegurarnos que tenemos una copia de seguridad actualizada de la información, al menos de aquella más crítica. Y comprobaremos que sabemos y que podemos recuperarla.
Carpetas de red compartidas sin control de acceso. Usuarios que no saben dónde está la última versión de un documento. Usuarios que tras un cambio de puesto conservan acceso a información que, por el nuevo tipo de trabajo que van a desempeñar, no es necesaria.	Estos errores se pueden evitar si hacemos que la información sólo sea accesible a quien la necesita y esté autorizado para ello. Es decir implantar un **«control de accesos»**.
Presencia de discos duros portátiles sin que la organización conozca y tenga inventariados quién los utiliza y qué información pueden tener almacenada. Falta de formación de los usuarios en las herramientas que utilizan. Dejar que los empleados utilicen almacenamiento en la nube y su correo personal para actividades profesionales	Si no se **limita el uso de aplicaciones no corporativas** (correo personal, almacenamiento en la nube) y se **controla el uso de los dispositivos externos** ni los usuarios tienen la adecuada formación, cometeremos estos errores.
Tirar los ordenadores y discos a la basura sin ningún control previo de su contenido.	Tener controlados los soportes y los equipos es esencial pues algún día dejan de ser útiles, por obsoletos o por desgaste. Es el momento de deshacerse de ellos, **borrar toda la información** que tenían, de forma que no quede ni rastro de su uso previo.

Tabla 1
Errores más comunes en el tratamiento de la información en la empresa

Aunque la tecnología es un elemento indispensable de cualquier organización, debe utilizarse de forma adecuada para evitar riesgos en la gestión de la información. Por tanto, es de extrema importancia que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad de la información.

3. DIMENSIONES DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de nuestra información:

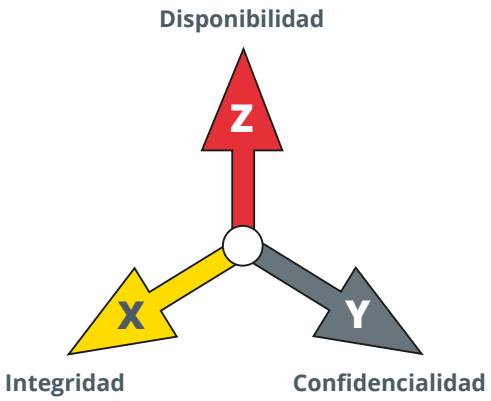


Ilustración 1
Dimensiones de la seguridad de la información

- **La disponibilidad** de la información hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.
- **La integridad** de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano.
- **La confidencialidad** implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como *need-to-know*. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso.

La evaluación de los activos de información de la organización en relación a estas tres dimensiones de la seguridad determina la dirección a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas.

También debemos tener en cuenta que la adopción de un determinado control para mejorar la seguridad en una dimensión, puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información. Por ejemplo, implantar un control de acceso para proteger la confidencialidad en un aparato médico de una sala de operaciones, puede producir un retardo en el acceso a la información afectando a su disponibilidad, lo cual no sería lo más adecuado.

4. SELECCIÓN DE SALVAGUARDAS

Las **salvaguardas** son las medidas necesarias para proteger la información de nuestro negocio.

Para la selección de estas medidas tendremos que fijarnos en los siguientes aspectos:

- Determinar la importancia de la información que manejamos. El **sector de negocio** puede afectar a la naturaleza de la información que tratamos, en particular en lo relativo a la privacidad de los datos personales de nuestros usuarios y por la existencia de información confidencial, cuya pérdida o deterioro pueda causar graves daños económicos o de imagen a la empresa.
- **Identificar, clasificar y valorar** la información según las dimensiones de seguridad son los pasos previos que van a dirigir la selección de las salvaguardas. Así, algunos activos de información serán muy confidenciales (estrategias, contraseñas,...), mientras que otros, como la página web o la tienda online, no podremos permitir que no estén disponibles.
- Tendremos también que conocer la **naturaleza de los controles** que podemos implantar. No sólo tendremos que considerar medidas técnicas como la instalación de un cortafuegos, sino que consideraremos también medidas organizativas, por ejemplo, implantar un plan de formación, establecer responsables de los activos o adaptarnos para cumplir con la legislación.
- El **coste** de las medidas será también un factor a considerar, pues ha de ser proporcional al riesgo **[1]** que se quiere evitar.

4.1. IMPORTANCIA DE LA INFORMACIÓN PARA LA EMPRESA

La importancia de la información que manejamos será, en gran medida, relativa a nuestro sector de negocio, así:

- En el **ámbito sanitario** se maneja un gran volumen de información personal de pacientes, a la que se deben aplicar todas las medidas de seguridad para evitar que se pierda, modifique o se acceda a ella sin autorización. Además suele ser necesario llevar un registro de los accesos y modificaciones.

- En **sectores industriales o de desarrollo de productos** es importante velar por la confidencialidad de los procesos y procedimientos que nos pueden aportar una mejora de productividad sobre la competencia.

- En el **sector financiero** se maneja información confidencial tanto de clientes como de operaciones financieras de compras y ventas de activos cuya difusión puede suponer una importante pérdida económica o un perjuicio para nuestros clientes.

- En **hostelería y restauración** se maneja, además de un volumen de datos de carácter personal muy significativo, información sobre reservas, cuya pérdida nos podría poner en una situación muy complicada con nuestros clientes.

La legislación sobre protección de datos de carácter personal **[2]**, define **datos personales** como «toda información sobre una persona física identificada o identificable (el interesado)». Una persona es identificable si puede determinarse su identidad, directa o indirectamente. Esta legislación exige la protección de la seguridad de los datos de carácter personal ante posibles riesgos que afecten a la privacidad de las personas por ejemplo: acceso no autorizado, uso ilegítimo, modificación no autorizada, discriminación por perfilado o pérdida de datos.

Existen categorías especiales de datos, los denominados datos sensibles que exigen una protección reforzada y que están sujetos a un régimen jurídico especial. Estos datos son:

- Datos personales que revelan ideología, afiliación sindical, opiniones políticas, creencias religiosas y otras creencias.
- Datos personales que revelan el origen racial o étnico y los relativos a la salud o la vida sexual y orientación sexual, datos genéticos y biométricos.
- Datos de condenas penales o administrativas.

La nueva legislación de protección de datos de carácter personal se basa en un **enfoque de riesgos** y en la responsabilidad proactiva. Esto implica que se han de aplicar las medidas técnicas y organizativas adecuadas y necesarias para garantizar los derechos y la privacidad de las personas cuyos datos personales tratemos, en base a un análisis de riesgos y para poder demostrarlo.

4.2. PASOS PREVIOS A LA SELECCIÓN DE SALVAGUARDAS

En primer lugar revisaremos qué información tratamos (bases de datos, archivos, aplicaciones, programas,...) y seleccionaremos la más crítica, la 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. En esta **clasificación de la información** podemos establecer varios niveles en función de su importancia para la empresa.

Este es un ejemplo orientativo **[3]** de cómo clasificar 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 a la misma únicamente a aquellos empleados que necesiten conocerla. 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 estar 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.

Tabla 2
Ejemplo clasificación información

Una vez hayamos clasificado y valorado la **criticidad** de la información, debemos determinar su riesgo específico para así enfocar las medidas a evitarlo o subsanarlo. Así, serán diferentes las medidas para evitar riesgos de fuga de información, de las necesarias para evitar que sea alterada por personas no autorizadas.

	Conocer la información que gestiona la organización. Esto debe hacerse a través de entrevistas y reuniones con el personal de la organización.
	Clasificarla según su criticidad, según un criterio razonable y unificado.
	Determinar su grado de seguridad: ¿es alto el riesgo de pérdida de información?, ¿y el de fuga o robo de información?, ¿puede ser alterada sin autorización?
	Establecer las medidas necesarias para mejorar su seguridad.

Ilustración 2
Pasos previos a la selección de medidas para proteger la información

En este punto se puede realizar un **análisis de riesgos** como se indica en la Guía de Gestión de Riesgos **[1]**. Este análisis permite valorar el coste de los posibles incidentes de seguridad que afecten a la información y priorizar las medidas que se tomen para evitarlos. Este análisis de riesgos será necesario si se tratan datos de carácter personal pues es esencial para determinar las medidas técnicas y organizativas necesarias para proteger la privacidad.

4.3. NATURALEZA DE LOS CONTROLES

Otro aspecto importante a considerar en la selección e implantación de controles es su tipología o naturaleza. Ésta puede ser:

- **Técnica:** medidas de carácter tecnológico dentro del ámbito de la seguridad. Son medidas técnicas: antivirus, cortafuegos o sistemas de copias de seguridad.
- **Organizativa:** medidas que se centran en la mejora de la seguridad teniendo en cuenta a las personas, por ejemplo: **formación** en seguridad, identificación de **responsables** o implantación de **procedimientos** formales de alta y baja de usuarios.
- **Física:** medidas físicas para proteger nuestra organización. Como por ejemplo, acondicionar adecuadamente la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados, establecer un sistema de control de acceso para entrar en las oficinas, poner cerraduras en los despachos y armarios o guardar las copias de seguridad en una caja ignífuga.

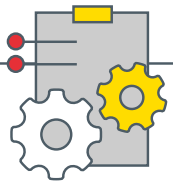
Se puede considerar también otro tipo de controles, los de naturaleza legal que persiguen el cumplimiento legal al que está sujeta la organización en el ámbito de la seguridad de la información.

4.4. RESUMEN DE CRITERIOS DE SELECCIÓN

Para escoger e implantar aquellos controles que nos ayuden a mejorar la seguridad de la información, tendremos que atender a:

El coste de la implantación de la medida de seguridad.

- Coste económico de la medida.
- Coste en el tiempo y recursos humanos empleados.
- Coste de las posibles medidas alternativas.
- Coste de las pérdidas económicas que supondrías no tener implantada la medida.



Las necesidades de cada sistema de información.

-Determinar cuál de las dimensiones de seguridad, confidencialidad, integridad o disponibilidad es más importante proteger.

La importancia de cada sistema de información en la organización.

- Identificar los activos más críticos e importantes a proteger.
- Contemplar las particularidades de cada sector de negocio.

Ámbito sanitario

Ámbito financiero

Ámbito industrial

Ámbito hostelería

Ilustración 3
Criterios selección salvaguardas

5. SALVAGUARDAS BÁSICAS

Existe un gran número de salvaguardas, definidas en múltiples estándares y normativas internacionales. Algunas de estas normativas, como la ISO 27002 **[5]**, son de carácter general, mientras que otras cubren ámbitos y propósitos específicos como por ejemplo, la continuidad del negocio.

Las medidas de seguridad a aplicar dependerán del tipo de sistemas a proteger, de la información que contienen, de las condiciones particulares de cada emplazamiento y de las amenazas a las que se exponen. A continuación mostramos aquellas que cualquier empresa debería tener en cuenta independientemente de su actividad.

5.1. CONTROL DE ACCESO A LA INFORMACIÓN

Por defecto, toda organización debe seguir el **principio del mínimo privilegio**. Este principio se traduce en que un usuario sólo debe tener acceso a aquella información estrictamente necesaria para desempeñar sus funciones diarias.

Para conseguir este objetivo, previo a la implementación de medidas técnicas o salvaguardas, debemos realizar los siguientes pasos:

- Definir los diferentes **tipos de información** que existen en nuestra organización: datos de recursos humanos, contabilidad, clientes, marketing, producción, etc.
- Establecer **quién puede acceder** a cada tipo de información. Para acometer esta tarea puede ser útil, si la estructura organizativa lo permite, realizar una matriz que cruce información con áreas o departamentos que tienen necesidad de acceso a dicha información (véase el ejemplo orientativo **[6]**).

	PERFILES DE LA INFORMACIÓN				
	Personal directivo	Personal de administración	Personal de informática	Personal operario	Personal de atención al cliente
Correo electrónico	✓	✓	✓	✓	✓
Nóminas	✗	✓	✗	✗	✗
Facturación	✓	✓	✗	✗	✓
Página web	✗	✓	✗	✗	✗
Servidor	✓	✓	✓	✗	✓
Pedidos	✓	✓	✗	✓	✓
Almacén	✗	✗	✗	✓	✗

Tabla 3
Ejemplo de perfiles y permisos sobre los activos de información

La asignación de permisos sobre los recursos que contienen la información puede realizarse **individualmente, por perfiles o por grupos de usuarios**. Tanto los sistemas Windows como los sistemas basados en Unix permiten asignar este tipo de permisos, de manera que se optimice su gestión.

Asignar permisos individualmente a cada usuario puede ser un método más flexible pero con mayor dificultad de gestión a medida que el número de usuarios crece.

Si optamos por asignar permisos según perfiles de usuario, será necesario llevar a cabo un mayor trabajo inicial para determinar a qué accede cada perfil y qué perfil tiene cada usuario, pero tras esta tarea inicial, la gestión de permisos es más rápida y eficiente, permitiendo una trazabilidad completa de los accesos de cada empleado.

- **Establecer quién y cómo debe autorizar el acceso** a los diferentes tipos de información. Es necesario responder, al menos, a las siguientes preguntas:

  - ¿Cómo se realiza la solicitud para acceder a una determinado tipo de información?, ¿a través de una aplicación de incidencias, un correo electrónico, un formulario en papel?
  - En el caso de utilizar alguno de los anteriores, ¿es suficiente con la solicitud electrónica, o es necesaria una firma manuscrita?
  - ¿Qué flujo seguirá la solicitud hasta que es autorizada o denegada?
  - ¿Quién tendrá permisos funcionales para autorizar o denegar el acceso?
  - ¿Quién realizará los cambios a nivel técnico?
  - ¿Será un acceso temporal o con permanencia en el tiempo?

Es vital escoger medios que permitan la **trazabilidad** y que sean proporcionales al volumen de información y tamaño de nuestra organización.

Debemos buscar un equilibrio para que, garantizando la seguridad, el acceso a una información por parte de un nuevo usuario autorizado se realice de manera ágil. Es importante evitar malas prácticas como el uso de «atajos» que aunque nos faciliten el trabajo supongan un problema de seguridad. Por ejemplo mover información de carpetas protegidas a otras no protegidas, lo que pueden suponer un control de accesos ineficaz, con graves consecuencias en la confidencialidad de la información.

Una vez hemos establecido **quién y cómo debe acceder a qué información**; y **quién y cómo debe autorizar ese acceso**; debemos garantizar que esto se cumple.

Para ello es imprescindible:

- Establecer mecanismos para revisar periódicamente que los permisos concedidos son adecuados, haciendo énfasis en los usuarios cuyos accesos han sido eliminados o modificados.
  - Comprobar, anualmente o con la periodicidad establecida en función de cada organización, la correcta asignación de los permisos. En caso de utilizar permisos por perfiles, verificar por un lado los permisos concedidos a cada perfil y por otro, los usuarios asignados a cada perfil.
  - Prestar especial atención a los servicios accesibles desde el exterior, como el uso del correo electrónico corporativo desde fuera de la empresa o el acceso de usuarios a nuestra infraestructura a través de VPN (red privada virtual).
- No limitarse al control de acceso lógico e incluir, cuando sea necesario, controles de acceso físico.

5.2. COPIAS DE SEGURIDAD

Las copias de seguridad son la salvaguarda básica para proteger la información. Dependiendo del tamaño y necesidades de la empresa, los soportes, la frecuencia y los procedimientos para realizar las copias de seguridad pueden ser distintos **[9]**.

Algunos soportes que podemos utilizar para la realización de copias son:

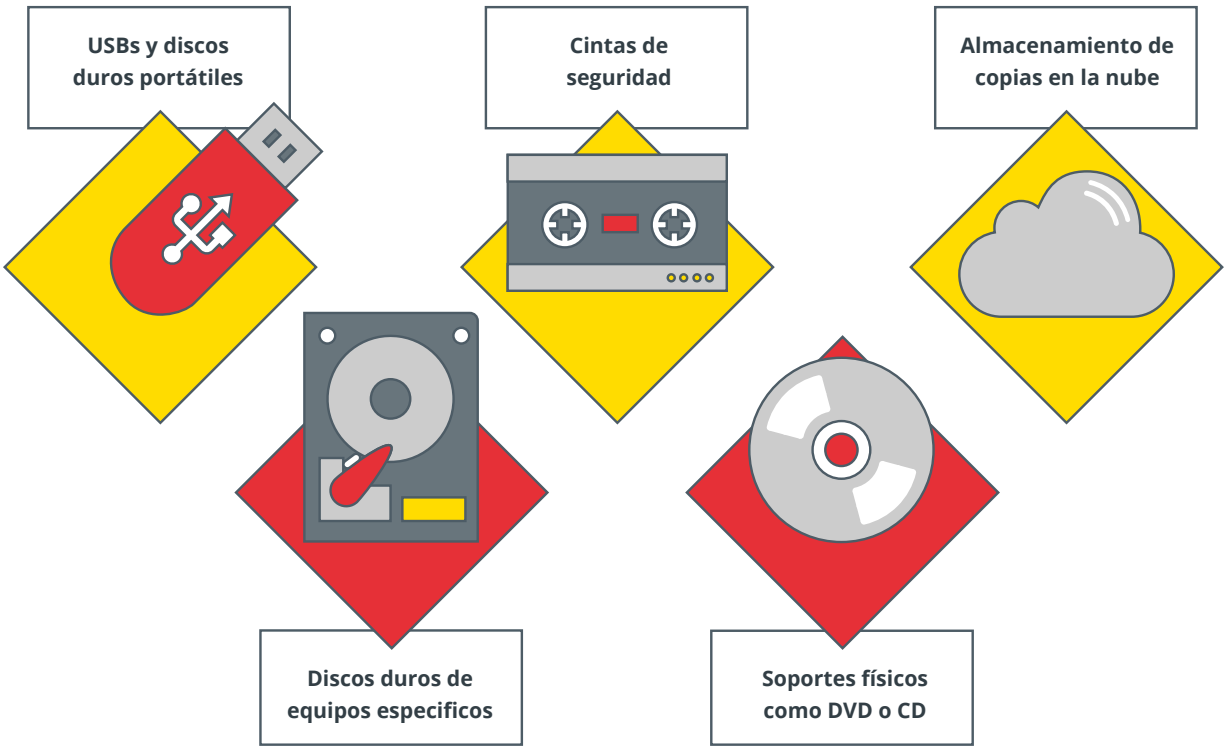


Ilustración 4
Soportes para realizar copias de seguridad

El soporte escogido dependerá del sistema de copia seleccionado, de la fiabilidad que sea necesaria y de la inversión que deseemos realizar. Estas tres variables van estrechamente unidas y deben estar en consonancia con la estrategia de nuestra organización.

En la implantación de un sistema de copias debemos tener en cuenta al menos las siguientes consideraciones:

- El primer paso es **analizar la información** de la que se va a realizar la copia, así como los sistemas y repositorios donde se encuentra. Debemos tener en cuenta aspectos como las configuraciones de dispositivos de red, los equipos de los usuarios o incluso información en *smartphones*. Este paso debe **permitirnos descartar información** sin relación directa con el negocio o ficheros históricos de los que ya existen copias.

- Debemos definir formalmente el número de versiones que vamos a almacenar de cada elemento guardado, y su periodo de conservación. Esto es lo que se conoce como política de copias de seguridad **[8]**.

  En esta decisión influyen las necesidades del negocio y la capacidad de almacenamiento disponible.

Una recomendación podría ser la siguiente:

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

En cualquier caso, la política dependerá de la complejidad de la organización y el volumen de los datos. Si el volumen de información es bajo, puede ser factible realizar una copia total diaria.

La principal diferencia entre la copia completa y los otros dos tipos de copia es la información que se almacena en cada iteración del proceso de copia de seguridad.

En **la copia total**, se realiza una copia completa y exacta de la información original, independientemente de las copias realizadas anteriormente.

En el caso de los sistemas de **copia incremental**, únicamente se copian los archivos que se hayan añadido o modificado desde la última copia realizada, sea total o incremental.

En el **sistema de copias diferenciales** cada vez que se realiza una copia de seguridad, se copian todos los archivos que hayan sido modificados desde la última copia completa.

- Deben hacerse **pruebas de restauración periódicas**, para garantizar que no se producirán problemas en caso de necesitar recuperar la información. Esto es especialmente importante si no se solicitan restauraciones con frecuencia. Los sistemas de copia o los soportes pueden fallar y es fundamental detectarlo antes de que sean necesarios.

  El método a utilizar para la restauración depende de la copia que utilicemos para reponer los datos.

En caso de utilizar la copia total, basta con reponer la totalidad de los datos contenidos en ella.

Pero si utilizamos **copias incrementales** para reponer la información necesitaremos la última copia total y todas las incrementales que se hayan realizado desde ese momento (ya que cada una de las copias incrementales contiene únicamente las diferencias con la anterior).

En caso de utilizar **copias diferenciales**, bastará con restaurar únicamente la copia total inicial y además la última copia diferencial disponible.

- Debe llevarse un **control de los soportes de copia**, mediante un etiquetado y un registro de la ubicación de los soportes. Las copias de seguridad tienen que estar en un lugar protegido, por ejemplo en un una caja ignífuga bajo llave. Esto implica también llevar el control de la vida útil de los mismos, para evitar que el deterioro físico afecte a la integridad de los datos.

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

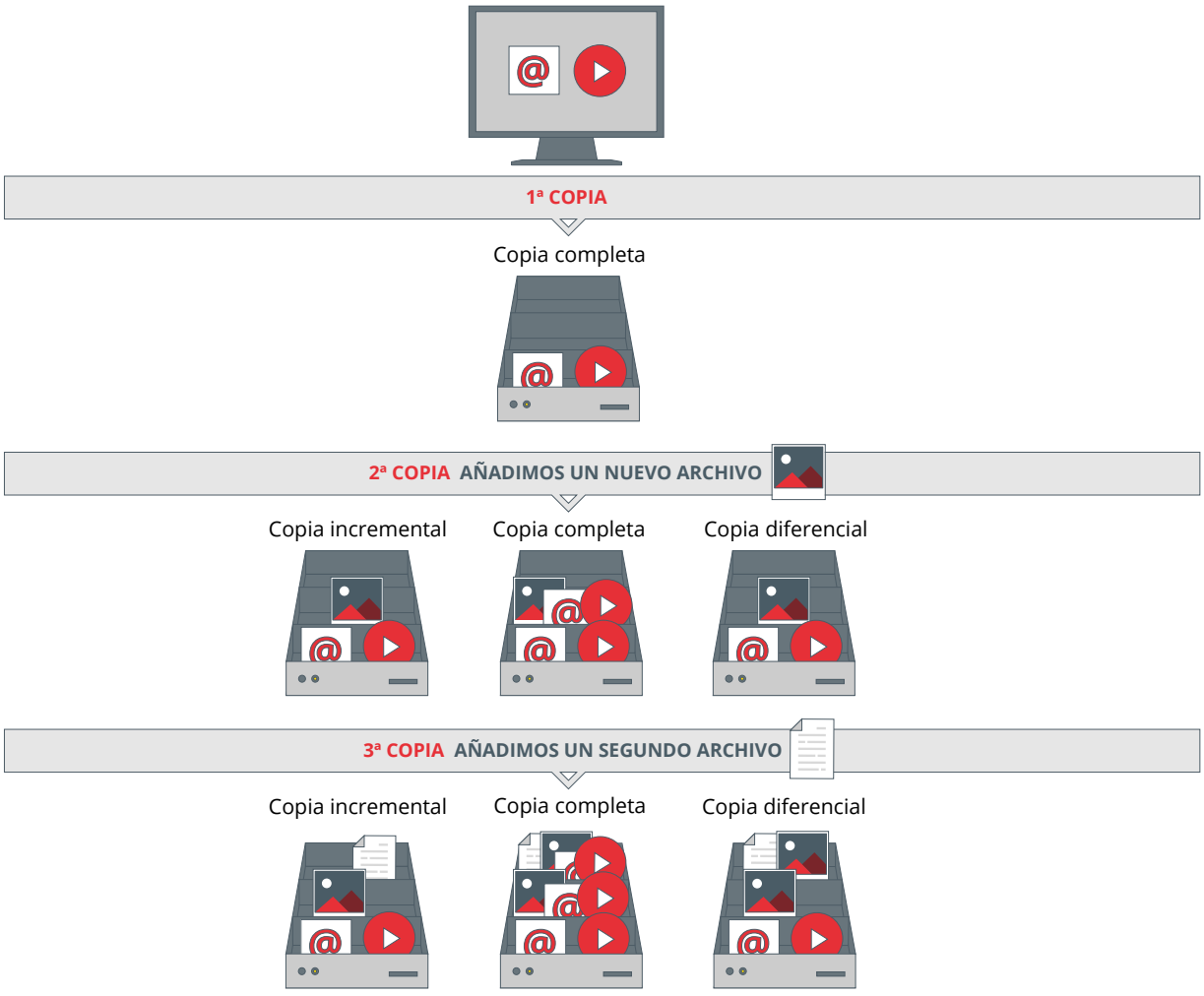


Ilustración 5
Tipos de copias de seguridad

- Si la información almacenada en las copias es confidencial, debemos valorar la **posibilidad de cifrarlas**, para evitar que ante una pérdida o sustracción de un soporte, sea posible acceder a ésta. Por ejemplo, se puede considerar información confidencial nuestros planes de negocio, la facturación de los clientes, ofertas que presentemos a clientes, datos de contabilidad, gastos y beneficios de la empresa, etc.

  Esta medida debe abordarse con especial cuidado para evitar la pérdida de información en caso de **pérdida de las claves**. Puede ser preferible que el cifrado se realice en el origen sobre archivos específicos y no en la copia de seguridad, especialmente en caso de utilizar servicios de almacenamiento «en la nube».

- Debemos disponer de una **copia de seguridad fuera de la organización**, para evitar la pérdida de la información en caso de incendio, inundación, robo o ser víctima de un malware que rastree nuestra red buscando estas copias de seguridad. Es necesaria una selección adecuada de **la localización de dichas copias**. Especialmente si decidimos realizar dicho almacenamiento en nuestro domicilio y éstas contienen datos de carácter personal, podemos estar infringiendo la legislación en materia de protección de datos. De manera alternativa y más segura, existen empresas de guarda y custodia que garantizan la seguridad de los soportes que les confiemos. Si utilizamos los servicios de otras empresas, el cifrado de la información puede servirnos para evitar el acceso no autorizado en caso de robo de la información.

- Por último, se debe **documentar** el proceso de realización y restauración de copias. Esto permitirá agilizar el proceso de recuperación ante una contingencia o ausencia del personal habitual.

- En caso de que utilicemos el almacenamiento en la **nube** para las copias de seguridad, debemos considerar la posibilidad de que no podamos acceder a la información de manera temporal, por un fallo del servicio o de nuestra conexión a Internet. Adicionalmente, deben considerarse los costes implicados y leer las políticas de privacidad y seguridad del servicio, especialmente si vamos a almacenar información con datos de carácter personal.

5.3. CIFRADO DE INFORMACIÓN

El cifrado consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean legibles por cualquier persona que desconozca la clave de decodificación. Estas técnicas son la mejor opción para el almacenamiento y transmisión de información sensible, especialmente a través de soportes y dispositivos móviles, ya que:

- permiten controlar el acceso a la información;
- limitan la difusión no autorizada en caso de pérdida o robo de soportes.

Sin embargo, hay que tener en cuenta una serie de aspectos:

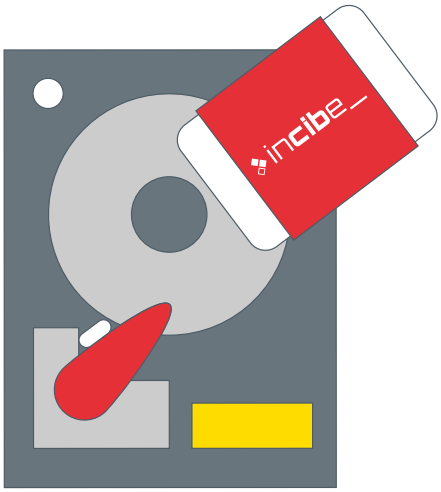
- la clave debe ser robusta para que dificultar el acceso no autorizado a la información;
- la **pérdida de la clave de acceso** imposibilita el acceso a la información;
- cuando ocurre un error físico no es posible la recuperación de la información, independientemente de si está cifrada o no.

La elección de la herramienta de cifrado dependerá de diversas variables:

- Si queremos una herramienta transparente al usuario o no.
- Si el descifrado de la información debe realizarse en cualquier lugar.
- El perfil del usuario que va a utilizar la herramienta de cifrado.

> Debemos tener en cuenta que para cifrar la información no siempre es necesario utilizar herramientas específicas. Programas habituales como las suites de ofimática o compresores de ficheros incorporan funcionalidades de cifrado para proteger la información.

5.4. DESECHADO Y REUTILIZACIÓN DE SOPORTES Y EQUIPOS



Antes de eliminar o reutilizar un soporte que haya almacenado información corporativa debemos aplicar las medidas de seguridad necesarias para evitar la recuperación de la información que previamente contuvieron.

Esto incluye los discos duros de los equipos, cintas de copias, discos magnéticos como CD y DVD, o memorias USB. A la hora de valorar los soportes de información, también debemos tener en cuenta la información que almacenamos en papel, que solemos desechar sin las adecuadas medidas de seguridad.

Existen dos medidas básicas en relación con la información que almacene el soporte, según su destino:

Existen dos medidas básicas en relación con la información que almacene el soporte, según su destino:

- Si vamos a **reutilizarlo, venderlo, regalarlo o prestarlo**, debemos realizar un **borrado seguro** del soporte. Es frecuente pensar que el borrado de la información o el formateo del disco duro elimina los datos, cuando no es cierto. Al eliminar archivos utilizando la función suprimir habitual del sistema operativo, éste se limita a marcarlo como eliminado. Pero los datos no han sido eliminados realmente. Siguen estando en el disco aunque el espacio que ocupaban aparezca como disponible. Y seguirán estando ahí hasta que nuevos datos ocupen esa zona de memoria.

  Existen multitud de herramientas que nos permiten borrar de forma segura los dispositivos. Estas herramientas de borrado seguro, además de marcar el espacio como vacío, escriben en él datos aleatorios un número determinado de veces. De este modo, si se intenta obtener el contenido anterior del disco duro lo que se encontrará serán datos aleatorios y no la información original.

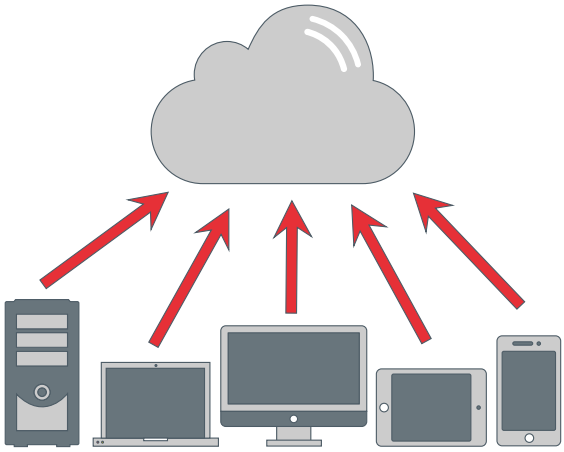
- Si por el contrario vamos a **desechar el soporte**, debemos garantizar que nadie puede utilizarlo posteriormente, y que la información que contiene no puede ser recuperada. Los soportes se pueden desechar por múltiples motivos, como pueden ser mal funcionamiento, poca capacidad, antigüedad o porque ya no es útil

  Por ejemplo, es frecuente que las memorias USB dejen de funcionar por algún fallo físico en el conector, pero la información almacenada esté intacta. Esto mismo puede ser aplicable a los discos duros.

  En general, la mejor opción es la **destrucción física del soporte**. Para los soportes menos robustos (CD/DVD, papel) podemos utilizar una destructora de papel (o de soportes magnéticos). Para otros medios, podemos optar por una destrucción manual o recurrir a empresas especializadas en la destrucción certificada de información.

Sea cual sea la opción escogida, siempre debemos asegurarnos que no será posible recuperar la información.

5.5. ALMACENAMIENTO EN LA NUBE



El almacenamiento en la nube hace referencia a los servicios de almacenamiento ofrecidos por distintos proveedores de Internet y que funcionan de manera similar a un disco duro remoto. Sus características básicas son la transparencia para el usuario y el acceso remoto desde cualquier lugar y dispositivo.

Este modelo proporciona varias **ventajas**:

- Reduce la necesidad de inversión en infraestructura propia.
- Permite delegar en terceros algunos aspectos que no forman parte de nuestro núcleo de negocio, como las copias de seguridad, su disponibilidad o la implantación de medidas de seguridad. Estos aspectos se controlan mediante los acuerdos de servicio con los proveedores que suelen incluir penalizaciones en caso de incumplimiento.

Sin embargo, este modelo no está exento de **riesgos**:

- No debemos utilizar servicios en la nube sin haber estudiado detenidamente las **condiciones de uso** en lo referente a las garantías de disponibilidad y confidencialidad de la información. Debemos informarnos sobre dónde acudir en caso de fallo del servicio, medidas de protección de la información, o los tiempos de indisponibilidad permitidos por contrato.
- Se debe evitar el **uso sin control** de estos servicios por parte de los empleados, mediante una política corporativa y medidas técnicas. El uso de estos entornos dificulta o imposibilita el control sobre la información que se almacena en el servicio, ya que las medidas de seguridad (control de acceso, claves utilizadas, registro de accesos) no están bajo el control de nuestra organización.
- En caso de manejar los datos de carácter personal, en particular si son datos especialmente protegidos, debemos tener en cuenta que tendremos que firmar con nuestros proveedores en la nube contratos de tratamiento de datos de conformidad con el RGPD **[2]**.

- Intentar evitar servicios en la nube que sean gratuitos. Cuando algo es gratuito, el producto somos nosotros, o nuestra información. Los servicios gratuitos en la nube ofrecen a menudo acuerdos de nivel de servicio inflexibles o con cláusulas ambiguas que no dejan nada claro cuáles son las medidas de seguridad que utilizan o la responsabilidad del proveedor.

No hay que olvidar que la utilización de almacenamiento en la nube implica que los datos pueden estar almacenados en cualquier lugar del mundo y no todos los países ofrecen las mismas garantías de seguridad y legales. Si contratamos este tipo de servicio para el almacenamiento para datos de carácter personal, seguimos siendo responsables del tratamiento de los mismos y debemos cumplir lo especificado por la legislación de protección de datos **[2]**. Aunque los principales proveedores disponen de acuerdos con la Unión Europea que permiten el almacenamiento de información personal en sus sistemas, debemos realizar un análisis previo de las garantías de privacidad antes de subir los datos al servicio.

Por otra parte existen servicios que permiten cifrar la información antes de «subirla a la nube», con las claves del servidor, a las que el usuario no tiene acceso para evitar que el proveedor o un atacante que comprometa la plataforma cloud tengan acceso a ella. También hay otros servicios que envían los datos ya cifrados siendo el usuario el único con acceso a los mismos. La solución más segura es cifrarlos y después subir la información a la plataforma *cloud*.

5.6. CONFIDENCIALIDAD EN LA CONTRATACIÓN DE SERVICIOS

Cualquiera de estos servicios es susceptible de ser externalizado: creación de las copias de seguridad, almacenamiento en la nube, destrucción física de soportes, mantenimiento informático, etc. Sin embargo, esta **externalización** puede introducir nuevos riesgos para la seguridad de la información, derivados del acceso del proveedor a los datos.

Una medida que mitiga (pero no elimina) este tipo de riesgo es la **firma de contratos de confidencialidad** o inclusión de este tipo de cláusulas en el contrato de servicio. Esto compromete al prestador del servicio a no hacer un uso fraudulento de los datos, y adquiere especial relevancia si se externaliza la gestión de datos de carácter personal ya que este acuerdo es un requisito legal obligatorio.

Para más información, puede consultarse el dossier de contratación de servicios **[7]**.

6. REFERENCIAS

[Ref - 1]. INCIBE, Guía de gestión de riesgos: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/gestion-riesgos-guia-empresario

[Ref - 2]. BOE. Legislación. Códigos. Protección de datos de carácter personal - https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2

[Ref - 3]. INCIBE, Protege tu información, «Matriz de clasificación de la información» - https://www.incibe.es/sites/default/files/contenidos/dosieres/proteccion-informacion/protege-tu-informacion-matriz-clasificacion-informacion.pdf

[Ref - 4]. UNE-EN ISO/IEC 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015) - https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0053761

[Ref - 5]. UNE-EN ISO/IEC 27002:2017 Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015) - https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0055190

[Ref - 6]. INCIBE, Protege tu información, «Ejemplo Clasificación de permisos por perfiles información» - https://www.incibe.es/sites/default/files/contenidos/dosieres/proteccion-informacion/protege-tu-informacion-ejemplo-permisos-perfiles-recursos.pdf

[Ref - 7]. INCIBE, Contratación de servicios - https://www.incibe.es/protege-tu-empresa/que-te-interesa/contratacion-servicios

[Ref - 8]. INCIBE, Herramientas – Políticas de seguridad para la pyme - https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[Ref - 9]. INCIBE, Copias de seguridad: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/copias-seguridad-guia-aproximacion-el-empresario

GOBIERNO
DE ESPAÑA
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege
tuempresa