Guía de **almacenamiento seguro** de la información

Una aproximación para el empresario

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2015
TRABAJANDO POR LA CONFIANZA DIGITAL

Guía de **almacenamiento seguro** de la información

Una aproximación para el empresario

INCIBE_PTE_AproxEmpresario_005_AlmacenamientoSeguro-2016-v1

índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 Introducción

Los recientes avances tecnológicos en Internet, las redes inalámbricas, los dispositivos móviles y la computación en la nube; junto a los servicios derivados de éstos como el comercio electrónico, la administración electrónica, los blogs, las redes sociales y las herramientas de colaboración, están transformando la forma de hacer negocios.

Las empresas basan su actividad en **sistemas de información**, en gran medida con soporte tecnológico. Estos sistemas manejan tanto información estructurada, por ejemplo en bases de datos, como información no estructurada en forma de documentos de texto, archivos de audio, videos o imágenes.

Desde otros puntos de vista la información se puede clasificar atendiendo a su función: operativa, táctica o estratégica.

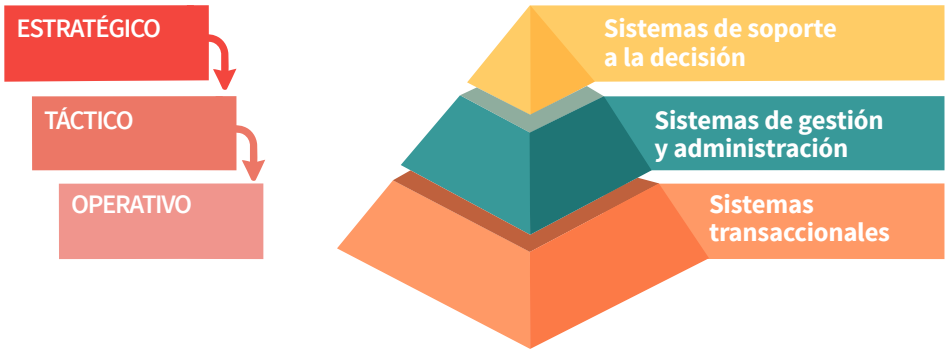


Ilustración 1: Sistemas de información en la empresa

Los sistemas de información están formados por elementos interrelacionados (hardware, software, comunicaciones, procesos y personas) que permiten transformar los datos en información y ésta en conocimiento, poniendo todo ello a disposición de los empleados y directivos de la organización para la toma de decisiones en los distintos niveles.

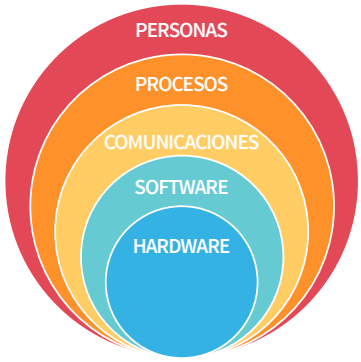


Ilustración 2: Elementos de los sistemas de Información

1 Introducción

«Las personas manejan información crítica que, de verse comprometida, puede interrumpir la actividad de la empresa»

En cuanto al software, —sólo un elemento más de estos sistemas—, se corresponde con todo tipo de programas y aplicaciones, desde los de ofimática y producción, hasta los de comunicación (correo electrónico, redes sociales) y el sitio web (CMS o gestores de contenidos web, comercio electrónico…), pasando por los de gestión y los de apoyo a la decisión, entre otros los denominados ERP (*Enterprise Resource Manager*), CRM (*Customer Resource Manager*) y los de apoyo a la decisión o BI (*Bussines Intelligence*).

Ilustración 3: Del dato al conocimiento

Con estos programas, las personas manejan (crean, comparten, transforman,…) información de clientes, de recursos humanos, de productos, de procesos, contable, financiera, estratégica, etc. Entre ella, **información crítica** que de verse comprometida, destruida o divulgada puede hacer tambalearse o incluso interrumpir la actividad de la empresa. Por ello la **gestión de la seguridad de la información** es necesaria para la buena marcha de cualquier negocio.

El establecimiento de procedimientos, planes y políticas **de almacenamiento, conservación, recuperación y borrado** es esencial para garantizar la seguridad de un activo tan importante para la empresa como la información.

El primer paso en la gestión segura de la información es realizar una **clasificación** de la información y garantizar un **almacenamiento** adecuado.

Son frecuentes las pérdidas de información por causas fortuitas, por fallos humanos o en los equipos. En este sentido, las técnicas de **recuperación** de la información son imprescindibles en las organizaciones, ya que permiten restaurar la actividad y asegurar su continuidad.

Cuando la información ha sido tratada en la empresa y llega al final de su vida útil, debe ser eliminada mediante procedimientos de **borrado seguro,** para evitar que pueda caer en manos de terceros y sea recuperada. El borrado seguro será objeto de otra guía.

Finalmente, la **conservación o archivado** de la información es un deber para determinadas actividades en las que los documentos generados pueden constituir evidencias o registros de hechos que han de justificarse o bien deben conservarse durante algunos años.

En la presente guía se analiza por qué se debe controlar la información en la empresa, cómo se almacena dicha información en los dispositivos de almacenamiento más comunes, cómo recuperarla en caso de que sea necesario y cómo conservarla.

1.1 La información como activo en la empresa

Las empresas manejan a diario gran cantidad de información y parte de esta información es más sensible, ya que es estratégica para el negocio, contiene datos personales de clientes, proveedores o empleados, tiene valor como propiedad intelectual, etc. Por este motivo, es imprescindible una adecuada **gestión de la información** que se maneja, tanto para asegurar la actividad del negocio como para cumplir con los requisitos legales que apliquen.

En el contexto de las normativas de gestión se entiende por **activo** aquello que tiene algún valor para la organización y por tanto debe protegerse. Los activos de información son, además de los soportes de la misma, todo tipo de información que posea valor para la empresa, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. Algunos ejemplos son: ficheros, bases de datos, contratos y acuerdos, facturas, documentación, manuales, aplicaciones, software, estadísticas, tráfico del sitio web, interacción en redes sociales, etc.

En este mismo contexto se define la **seguridad de la información** como la preservación de la confidencialidad, la integridad y la disponibilidad de los activos de información.

Por tanto a la hora de confirmar que el modo en que se trata la información es seguro hay que considerar tres dimensiones: el grado de **confidencialidad,** la **integridad** y el nivel de **disponibilidad.**

- **Confidencialidad:** por la cual la información no debe ponerse a disposición o revelarse a individuos, entidades o procesos no autorizados
- **Integridad:** por la cual la información debe poder conservar su exactitud y completitud
- **Disponibilidad:** por la cual la información debe estar accesible y utilizable por las entidades (usuarios, procesos…) autorizadas

Ilustración 4: Propiedades de la información desde el enfoque de la seguridad

1 Introducción

«El tratamiento de la información personal está regulado por ley y su incumplimiento puede acarrear sanciones legales»

En algunos contextos, se pueden tener en cuenta por su importancia otras propiedades de la seguridad de la información como son la responsabilidad y el no repudio. Por ejemplo en el caso de las transacciones (apuntes en una cuenta bancaria, entradas y salidas de almacén…) es importante considerar la **responsabilidad** o rendición de cuentas, es decir, la capacidad de justificar qué ha ocurrido, quién lo ha hecho y cuándo. Si se trata de la transmisión de mensajes, por ejemplo por correo electrónico, es importante también el **«no repudio»,** es decir poder certificar el origen, dónde se generó el mensaje, o el destino, a dónde ha llegado.

Dada la trascendencia de la información como base para la toma de decisiones estratégicas y su relevancia a la hora de establecer ventajas competitivas, es necesario contar con una eficiente **gestión de la seguridad** que preste especial atención a este recurso, a lo largo de todo su ciclo de vida desde que se crea hasta que se destruye de forma definitiva.

Estas son algunas de las situaciones que una correcta gestión de la seguridad de la información quiere evitar:

- Los equipos y soportes que utilizamos para almacenar la información (móviles, portátiles, discos externos, pendrives…) pueden ser extraviados o robados, con la consecuente **pérdida o robo** de información que contienen.

- Las comunicaciones, tanto por correo electrónico como por otros medios como redes sociales, pueden ser el origen de la **difusión indebida de información confidencial,** incluidas contraseñas y credenciales de acceso por desconocimiento, error o con intención.

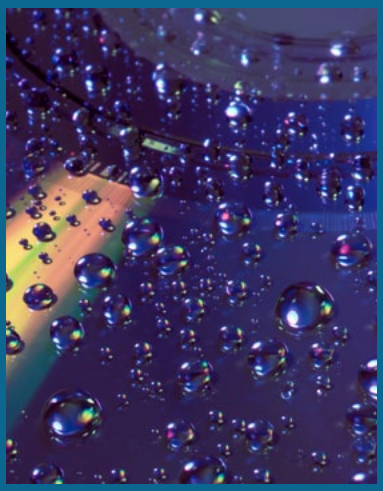
- El acceso por personas no autorizadas a la información puede dar lugar a la consiguiente **destrucción, manipulación o difusión no autorizadas.** Por ejemplo los datos que registran transacciones, de ser accedidos por personas no autorizadas, pueden ser alterados o destruidos y resultar inservibles para justificar acciones realizadas.

- El tratamiento de la información personal está regulado por la ley y su no cumplimiento puede acarrear **sanciones legales.**

- Empleados o usuarios sin mala intención, por descuido o por caer en los engaños de la ingeniería social, pueden **divulgar o destruir información sensible o de carácter personal, incluso credenciales de acceso** que pueden llevar a **intrusión en sistemas,** daños de imagen o tener consecuencias legales.

- Los soportes y equipos que han dejado de utilizarse contienen información que debe borrarse o destruirse pues puede llegar a terceros y acarrear, si se divulgan, **daños de imagen,** consecuencias legales, etc.

1 Introducción



«Si no se hacen copias de seguridad no podremos recuperar la información en caso de incidentes o desastres»

También puede ocasionar **daños de imagen** la manipulación de contenidos en nuestra web o de nuestra tienda online (precios, productos…) por personas no autorizadas que puedan acceder al gestor de contenidos. Esto puede ocurrir si llegan a sus manos las credenciales de acceso al mismo por ejemplo por descuido o por estar infectado con malware.

La información almacenada en sistemas de **almacenamiento compartido o en la nube** puede ser manipulada, destruida o divulgada si no se toman las mismas medidas para garantizar su seguridad (control de acceso, cifrado…) que para el almacenamiento en local.

En caso de **desastre natural,** si las copias de seguridad se almacenan en la misma oficina, pueden resultar destruidas como el resto de los equipos y hacer imposible su recuperación. Si no se hacen copias de seguridad tampoco podremos recuperar los sistemas en caso de incidentes o desastres.

Los soportes se deterioran con el tiempo, las partes mecánicas pueden fallar pudiendo dejar inaccesible la información que contienen.

El software que trata la información puede tener **vulnerabilidades** y, si no se actualiza con frecuencia, podría ser objeto de todo tipo de ataques, accesos no autorizados, infecciones con malware, etc.

Los dispositivos personales, móviles y tabletas con sus apps, que se usan para acceder a recursos de la empresa, de no estar correctamente configurados, pueden dar lugar a **fugas de información.**

2 Clasificación de la información

Atendiendo a la importancia de los distintos activos de información para la empresa, se ha de llevar a cabo una **clasificación** que permita aplicar a la misma las medidas de seguridad oportunas. Para la clasificación se pueden considerar, además de su antigüedad y valor estratégico, las tres propiedades: confidencialidad, integridad y disponibilidad.

Lo más usual es clasificar la información teniendo en cuenta solamente una de estas tres dimensiones, la confidencialidad. Se clasifica la información en tres niveles: confidencial, de uso interno e información pública. Esta aproximación es la más aceptada, pues uno de los riesgos más críticos para cualquier negocio es la fuga de información [1] que no es más que una pérdida de la confidencialidad de la misma.

A continuación se presenta una posible clasificación 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. • Se incluye la información que contenga datos de carácter personal de nivel alto.	• 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 nivel alto, se deben cumplir también las medidas de seguridad indicadas en el Reglamento de Desarrollo de la LOPD.
Interna	• Información propia de la empresa, accesible para todos los 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 marcarse adecuadamente 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 1: Ejemplo de clasificación de la información

No obstante, en función del carácter de la empresa, no hay que descuidar otras dimensiones de la información, ya que pueden ser muy relevantes para el negocio. Imaginemos por ejemplo una empresa financiera para la cual la **integridad** de las transacciones es un aspecto esencial, o las empresas con tienda online en las que su **disponibilidad** es un factor

«La Agencia Española de Protección de Datos es la autoridad pública encargada de velar por la privacidad y la protección de datos de los ciudadanos»

crítico de negocio. Igualmente relevantes pueden ser la **responsabilidad** y **el no repudio,** por ejemplo en el caso de gestorías que deban rendir cuentas de sus actividades o para abogados y notarios que deban certificar el origen y destino de sus comunicaciones.

Un caso especial a tener en cuenta son los **datos de carácter personal,** es decir, los que afectan a la **privacidad** de los individuos. Por ejemplo los datos que se almacenan en bases de datos sobre clientes y proveedores, incluidos los ficheros de credenciales de acceso, las cookies que almacenan las páginas web o los datos de las cámaras de video vigilancia, están regulados por la Ley de Protección de Datos, la LOPD [2]. Para estos datos, dependiendo de su clasificación, la Ley establece tres niveles de protección. Así, los datos personales más sensibles (datos de salud, ideología, etc.) deben estar más protegidos. La Agencia Española de Protección de Datos, AEPD [3] es la autoridad pública encargada de velar por la privacidad y la protección de datos de los ciudadanos. Este organismo dispone de guías [4] dónde consultar los niveles de protección de este tipo de datos y las medidas de seguridad (control de acceso, gestión de soportes, registro de incidencias, cifrado, destrucción segura…) que deben aplicarse en cada caso.

Otra información que merece un tratamiento singular es la relativa a patentes, modelos de aplicación, marcas y diseños industriales. Está regulada por la legislación sobre propiedad industrial [5]. Otras empresas, en particular las empresas de contenidos digitales, tendrán que contar con las medidas adecuadas para las creaciones artísticas o literarias propias o ajenas según lo regulado por la legislación de propiedad intelectual [6].

Por esto es importante identificar toda la información que se maneja, **incluido el software, sin importar el soporte o su formato.** Se ha de registrar su ubicación y la persona o equipo responsable y clasificarla según los criterios de seguridad que sean más adecuados, incluidas las necesidades de cumplimiento legal que sean aplicables, según la actividad de la empresa. Esta clasificación será esencial para aplicar las medidas de seguridad adaptadas a la criticidad de cada «clase» de información para el negocio.

Una vez clasificada, aplicaremos las medidas necesarias para su protección. Estas medidas, que se concretarán en distintas políticas, se dirigen a definir:

- Ubicaciones y dispositivos permitidos para el almacenamiento y uso de la información según su criticidad.
- Cifrado de información crítica en tránsito o en almacenamiento.
- Control de acceso a la información almacenada y a los servicios y programas para su tratamiento; permisos por roles, contraseñas robustas…
- Control de uso de dispositivos externos de almacenamiento y de móviles o tabletas.

2 Clasificación de la información

«Es importante identificar toda la información que se maneja y clasificarla según los criterios de seguridad»

- Control del uso de almacenamiento y servicios en la nube.
- Destrucción segura de la información una vez terminada su vida útil (otra guía tratará la forma de conseguir una destrucción segura).
- Copias de seguridad y planes de recuperación.
- Según la actividad de la empresa, archivado seguro de la información que se deba conservar y de los registros de actividad como garantía del cumplimento legal o normativo que aplique.

3 Almacenamiento de la información

La creciente dependencia de la mayoría de las organizaciones de sus sistemas de información pone de manifiesto la necesidad de contar con medios y técnicas que permitan almacenar la información de la manera más adecuada. Una correcta gestión de este proceso permite mantener en todo momento la integridad, confidencialidad y disponibilidad de la información.

3.1 Cómo se almacena la información

Las empresas necesitan infraestructuras de almacenamiento flexibles y soluciones que protejan y resguarden la información y se adapten a los rápidos cambios del negocio y las nuevas exigencias del mercado, garantizando el rápido retorno de la inversión efectuada. Alineando las diferentes soluciones de almacenamiento con los requerimientos del negocio se consigue hacer un uso más correcto de las mismas.

En la siguiente ilustración se identifican los diferentes sistemas de almacenamiento de información en la empresa.

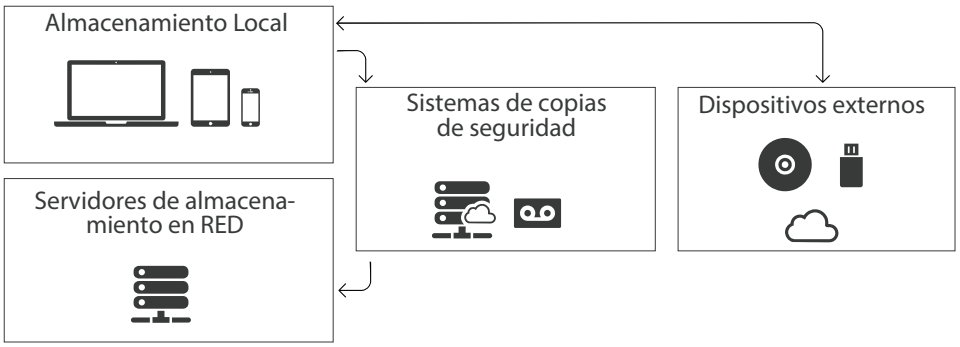


Ilustración 5: Sistemas de almacenamiento en la empresa

Almacenamiento local. Los empleados de la empresa utilizan equipos informáticos para realizar su actividad profesional. La información se genera en estos equipos y desde ellos se modifica y transmite. Cada uno de estos equipos dispone de un sistema de almacenamiento local, normalmente discos duros donde se guarda la información. También es almacenamiento local el utilizado en tabletas y dispositivos móviles interno o en tarjetas de memoria (micro SD).

Servidores de almacenamiento en red. Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre los diferentes usuarios de la empresa se dispone de servidores de almacenamiento en red.

Dispositivos externos. Adicionalmente se puede disponer de sistemas externos que, conectados directamente a los equipos, permiten un almacenamiento extra de la información, evitando que se ocupe este espacio en el equipo. Estos pueden ser cintas magnéticas, discos duros externos, CD o DVD o pendrives conectados a través de distintos interfaces físicos. Existen también dispositivos externos que se pueden conectar de forma inalámbrica. Los distintos tipos de interfaz tienen también distinta velocidad de transferencia. Por su portabilidad es fácil que se puedan extraviar.

«Se recomienda establecer un procedimiento para sistematizar la realización de copias de respaldo de la información generada en la empresa»

Sistema de copias de seguridad [7]. Es muy recomendable establecer un procedimiento para sistematizar la realización de copias de respaldo de la información generada en la empresa, en soportes externos o en otra ubicación. Algunas empresas optarán por sistemas de respaldo de toda o parte de su sistema de información, de manera que puedan continuar su actividad en caso de desastre.

Servicios de almacenamiento en la nube. Es posible utilizar servicios de almacenamiento en la nube [8] como medio de almacenamiento externo, para compartir la información generada o para realizar copias de seguridad. Un caso particular de almacenamiento es el asociado a la contratación de servicios externos como servicios de **backup, alojamiento web o las tiendas online.** Al contratar servicios en la nube se deben seguir los mismos criterios de seguridad de la empresa para la información asociada a los servicios contratados, reflejándolo en los **Acuerdos de Nivel de Servicio** [9] que se firmen con los proveedores.

3.2 Tipos de dispositivos de almacenamiento

Los dispositivos de almacenamiento constituyen una parte vital de cualquier sistema o instalación informática. La tendencia general en el mercado de los dispositivos de almacenamiento de información se dirige, por un lado, al continuo incremento de su capacidad y, por otro, a desarrollar funcionalidades como la rapidez, la fiabilidad, la economía y el tamaño. Esta evolución se traduce en una disminución del coste, lo que ha permitido aumentar el número de empresas que utilizan estos dispositivos.

La gama es amplia y las funcionalidades dependen del tipo de dispositivo, aunque como aproximación, se indican los siguientes:

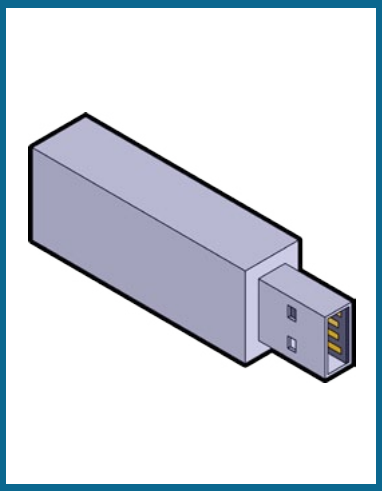
Discos duros (HDD y SSD): dispositivo de almacenamiento utilizado en todos los ordenadores como almacenamiento principal. Los HDD son discos duros magnéticos[1] y llevan piezas mecánicas. Los SSD, discos de estado sólido, son electrónicos, más rápidos y silenciosos pero de menor capacidad. En ambos casos se pueden encontrar de distintas capacidades de almacenamiento y permiten tanto la lectura como la escritura. Los discos duros también se utilizan como medios de almacenamiento externos conectados a los equipos por medio de conectores USB (*Universal Serial Bus* o conductor universal en serie), eSATA, Firewire o Thunderbolt. En el mercado también hay discos duros que se conectan de forma inalámbrica.

Cintas magnéticas DAT/DDS (*Digital Audio Tape/Digital Data Storage*) / LTO (*Linear Tape-Open*): utilizadas principalmente como medio de almacenamiento en los sistemas de copias de seguridad, ya que resultan económicas para almacenar grandes cantidades de datos. El acceso a los datos es sensiblemente más lento que el de los discos duros.

1 Los dispositivos de almacenamiento magnéticos son aquellos cuyo soporte de almacenamiento lo componen unas partículas que pueden polarizarse en un sentido u otro según la dirección de un campo magnético aplicado a ellas. La dirección de polarización de sus partículas indicará si el dato almacenado es un uno o un cero.

3

Almacenamiento de la información



«Las memorias USB son especialmente susceptibles a la pérdida de información»

CD (*Compact Disc*) / DVD (*Digital Versatile Disc*) / Blu-ray Disc (*BD*): dispositivos de almacenamiento óptico con diferentes capacidades de almacenamiento. Son un medio económico y fácil de transportar o conservar. También al ser dispositivos que permiten una escritura y muchas lecturas, son adecuados para hacer copias de seguridad anti-*ransomware*, es decir, que no podrán ser secuestradas por malware que pida rescate para su recuperación.

Sistemas de almacenamiento en red: las empresas que necesitan almacenar gran cantidad de información utilizarán los sistemas de almacenamiento en redes del tipo NAS (*Network Attached Storage*), para archivos compartidos, o SAN (*Storage Area Network*) de alta velocidad para bases de datos de aplicaciones. Presentan un volumen de almacenamiento grande, ya que unen la capacidad de múltiples discos duros en la red local como un volumen único de almacenamiento. Las reglas de acceso permiten llevar un control de quién tiene acceso y a qué partes de la información almacenada se tiene acceso.

Memorias USB y USB-OTG: denominado con múltiples nombres como llavero USB, memoria USB o pendrive. Es un pequeño dispositivo de almacenamiento que dispone de una memoria electrónica de altas prestaciones para el almacenamiento de la información. La capacidad de los pendrives es cada vez mayor y es uno de los medios más utilizados para transportar la información de un lugar a otro. Esta movilidad, unida a la rapidez con la que se conecta y desconecta en diferentes equipos, lo hace especialmente susceptible a la pérdida de información, por extravío o sustracción del dispositivo o por rotura física del mismo.

En general para adquirir un dispositivo de almacenamiento se ha de tener en cuenta, además del precio y del tamaño, estas consideraciones:

Capacidad de almacenamiento (en GB[2], TB[3] …) adecuada a nuestras necesidades.

Compatibilidad del sistema de archivos, el formato lógico en el que se almacena la información, con nuestro sistema operativo. Por ejemplo NTFS y FAT en Windows o HFS y HFS+ para Mac OS.

Compatibilidad del interfaz de conexión (USB 2.0, 3.0…) con el de nuestro sistema.

Velocidad de transferencia (Kb/s, Mb/s); y si tiene o no caché o buffer, una memoria de intercambio que agiliza la transferencia, en el caso de discos duros.

Tipo de almacenamiento, ya que influye en la velocidad de acceso (óptico, magnético o electrónico) y si tiene partes mecánicas, como los HDD, por el ruido que pueda producir y por la necesidad de algún tipo de mantenimiento.

2 GigaByte o 10^9 (mil millones) bytes. Un Byte u octeto es una unidad de información que generalmente está formada por 8 bits (unidad básica de codificación de la información que puede tener dos valores 0 y 1). En la mayoría de las arquitecturas de ordenadores se utiliza 1 Byte para codificar cada carácter.
3 TeraByte o 10^{12} (un billón) bytes.

4 Pérdida y recuperación de la información

La información es un activo de valor para la empresa y, como tal, la posibilidad de que ésta pase a manos no autorizadas, o que no esté disponible, puede tener repercusiones importantes para la empresa.

En caso de que se produzca una pérdida de datos temporal o definitiva, se ocasionan múltiples **perjuicios** al funcionamiento de la empresa, por ejemplo:

- Pérdidas económicas:
  - El tiempo y dinero perdidos por los procesos llevados a cabo para restaurar o volver a generar la información perdida
  - Las pérdidas ocasionadas por la indisponibilidad de esta información, como pueden ser los retrasos en los procesos de producción
  - La pérdida definitiva de trabajos y proyectos ya realizados, que puede llegar a poner en riesgo la continuidad del negocio
- Pérdida o daño de imagen:
  - En caso de tener que solicitar de nuevo información a clientes o proveedores
  - En el caso de pérdida de datos de clientes que pueda poner en riesgo su privacidad
  - Por la publicación de datos privados en medios y por la difusión del incidente
- Demandas o penalizaciones administrativas por posibles incumplimientos de contratos o legales en el caso de pérdida de datos personales

En los siguientes apartados se analiza tanto la pérdida de la información como la posibilidad de recuperación de la misma.

4.1 Pérdida de información

El objetivo básico de un dispositivo de almacenamiento es guardar información para que esté disponible posteriormente. Para ello todos los componentes físicos del dispositivo tienen que funcionar correctamente y el sistema operativo debe encontrar la información que ha sido almacenada de un modo ordenado. Al guardar cada archivo, se anota también su ubicación en una base de datos o «lista de archivos[4]». Esta lista es el índice que utiliza el sistema operativo para encontrar el contenido de los archivos dentro del disco.

Se dice que se produce una pérdida de información o datos cuando se altera alguno de sus atributos de integridad, disponibilidad y confidencialidad y, específicamente en el proceso del almacenamiento, la disponibilidad es el atributo más crítico. Una información se pierde definitivamente cuando no se consigue el acceso a la misma o ésta ha desaparecido.

4 La «lista de archivos» es un término genérico que referencia al conjunto de elementos que cada sistema de archivos utiliza para guardar, tanto la información que identifica los archivos (nombre, tipo, fecha de creación, etc.), como un índice que recoge la ubicación física del contenido del mismo.

«Las acciones precipitadas sobre los dispositivos en un intento de recuperación pueden llevar a la destrucción definitiva de los datos»

4.1.1 Causas de la pérdida de datos

Las causas por las cuales se producen las **pérdidas de acceso** a la información, afectando tanto a su integridad como a su disponibilidad, son múltiples y en muchos casos previsibles. Entre ellas destacan las siguientes:

- **Fallos mecánicos en los dispositivos de almacenamiento:** causados bien por motivos externos (como cortes de suministro eléctrico o picos de tensión en la red eléctrica), o internos de los propios dispositivos (por ejemplo, por degradación de las piezas mecánicas al final de la vida útil de los mismos).

- **Errores humanos:** por borrado o formateo de las unidades de almacenamiento o por manipulación indebida de los dispositivos. A veces la mala preparación del personal y la toma de decisiones erróneas a la hora de intentar recuperar la información tras un incidente son las causas de estos errores.

- **Fallos en el software utilizado:** fallos imprevistos en los sistemas operativos por reinicios inesperados o mal funcionamiento de las propias herramientas de diagnóstico.

- **Virus o software malicioso:** ya que en ocasiones los programas instalados en los ordenadores buscan causar un fallo en el sistema o bien el deterioro o el robo de información enviándola a un equipo remoto.

- **Desastres naturales o estructurales:** como incendios e inundaciones que causan la destrucción de las instalaciones donde se encuentran los equipos.

- Las causas por las cuales se producen las **pérdidas de confidencialidad** y sus consecuencias se tratan con detalle en la Guía «Cómo gestionar una fuga de información: una aproximación para el empresario» [1].

4.1.2 Recomendaciones ante una pérdida de datos

Cuando un disco duro se rompe y no se puede acceder a los datos que contiene, se habrán perdido los datos si no se dispone de una copia de estos mismos datos en otro dispositivo al cual sí se pueda acceder. Por tanto, primer consejo: se debe disponer y seguir una correcta **política de copias de seguridad.**

Además, ante un incidente de pérdida de datos se recomienda:

- Evitar actuar de una forma precipitada. Las acciones sobre los dispositivos que se realicen en un intento desordenado de recuperación pueden llevar a la destrucción definitiva de los datos.

- No reiniciar constantemente el dispositivo, ya que esto puede agravar el daño que sufra en caso que éste tenga algún fallo físico de funcionamiento.

«La pérdida de información puede no ser definitiva si existen medios para restaurar la disponibilidad de acceso»

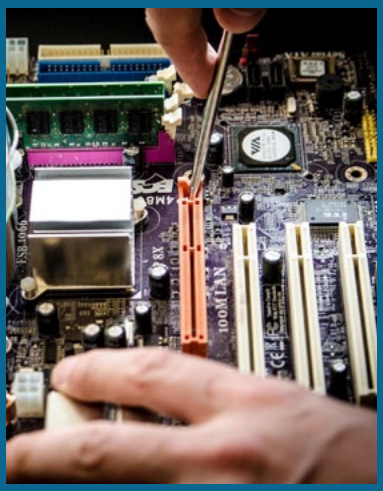
- Dedicar un tiempo a analizar cuáles son los datos perdidos, si se dispone de una copia de seguridad y el estado de la misma.
- Valorar la pérdida, tanto económica como de tiempo de restauración, para ver con más claridad la dimensión del problema y los medios que se pueden dedicar a la restauración de los datos.
- Decidir si es mejor iniciar un proceso de recuperación de datos o restaurar el sistema y generar de nuevo los datos perdidos.
- Si se intenta restaurar la copia de seguridad no es aconsejable utilizar los discos «dañados» para recuperar los datos de la copia. En caso de que la copia restaurada no se encuentre totalmente operativa o esté desactualizada, no se podrá intentar una recuperación posterior. Igualmente hay que tener especial cuidado para no realizar ninguna acción que pueda sobre-escribir los datos en el soporte «dañado».
- Cuando la pérdida de datos se produce en sistemas compuestos por varios discos, es recomendable que al menos dos personas realicen el seguimiento de las decisiones para poder contrastar que la decisión tomada es la adecuada, y que se anotan todos los pasos realizados.
- No es recomendable desmontar los dispositivos sin tener un conocimiento profesional, ya que dicha acción puede ocasionar la imposibilidad de recuperación posterior.

4.2 Recuperación de la información

Si se ha perdido el acceso a una información almacenada, dicha pérdida puede no ser definitiva si existen medios para restaurar la disponibilidad de acceso, en cuyo caso se puede plantear la recuperación de la información. El acceso a la información se puede perder por varios motivos, como son:

- Porque el dispositivo tiene dañado algún componente físico necesario para su funcionamiento
- Porque, aún funcionando correctamente, la «lista de archivos» se ha corrompido impidiendo conocer la ubicación de los archivos almacenados
- Porque los datos almacenados han sido reemplazados por nuevos datos por sobreescritura

En los dos primeros casos se puede intentar un proceso de recuperación, en el tercero no puede realizarse ya que esos datos ya no existen y por tanto no pueden recuperarse.



«Se desaconseja totalmente el intento de recuperación física de un dispositivo por personal no experto»

4.2.1 Métodos de recuperación de la información

Por métodos de recuperación de datos se entienden aquellos procesos llevados a cabo con el objetivo de restablecer el acceso a la información que sigue estando almacenada en los dispositivos, pero que no está disponible por alguna de las causas señaladas anteriormente. Los métodos de recuperación son:

1. Métodos de recuperación lógica. Los métodos de recuperación lógica se utilizan cuando todos los componentes del dispositivo funcionan correctamente y por tanto se puede acceder a todos y cada uno de los sectores donde se almacena la información. Si se ha perdido acceso a los datos podrá ser debido a que:

- Alguna parte de la estructura del sistema de archivos se encuentra dañada
- Algún archivo ha sido borrado con los comandos del sistema y por tanto no aparece en la «lista de archivos» que contiene el sistema

La recuperación lógica de datos consiste en analizar la estructura de archivos que permanece, identificar el daño producido y acceder a los datos que aún están en el dispositivo. En algunos casos se pueden recuperar los datos identificativos del archivo, (nombre, extensión, tamaño, fecha de creación, etc.) y en otros sólo el contenido del mismo.

Algunas herramientas[5] emplean el término análisis profundo o «en bruto» que consiste en analizar toda la superficie del disco buscando aquellas codificaciones específicas que permiten identificar a cada tipo de archivo y recuperan directamente el contenido de los mismos, sin tener en cuenta la información presente en la «lista de archivos», por lo que se pierden el nombre y las fechas de los archivos recuperados. Las herramientas de reparación de sistemas de archivos que disponen los sistemas operativos tales como «chkdsk» en sistemas Windows, «fsck» en sistemas Linux o las utilidades de disco en Mac OS pueden reparar algunos errores de los sistemas de archivos. Sin embargo, un conocimiento insuficiente puede provocar daños mayores al sistema y hacer irrecuperable la información. Por ello, es recomendable acudir a profesionales en recuperación de datos ante una situación de este tipo.

2. Métodos de recuperación física. Si algún componente físico del dispositivo se encuentra dañado, pero el soporte de almacenamiento sigue inalterado, se podrá abordar una recuperación física reparando o sustituyendo el componente dañado y accediendo nuevamente a la información guardada.

Los métodos de recuperación física requieren un conocimiento de cada uno de los dispositivos y se desaconseja totalmente el intento de recuperación por personal no experto.

5 Algunas aplicaciones gratuitas que utilizan análisis en bruto son: PhotoRec http://www.cgsecurity.org/wiki/PhotoRec_ES y Recuva https://www.piriform.com/recuva (esta última sólo para Windows).

5 Conservación de la información

Conservar la documentación a medio-largo plazo es una actividad necesaria para algunas empresas por motivos administrativos o legales o por el carácter de la información (resultados de investigaciones científicas, obras de arte, etc.).

En cualquier negocio hay documentos que deben conservarse durante algún tiempo, incluso después del cese de actividad de la empresa. Por ejemplo los documentos contables deben conservarse durante seis años y las declaraciones de impuestos durante cuatro.

Otros documentos pueden precisar trazabilidad, a menudo proporcionada por terceros de confianza, por ejemplo las facturas electrónicas [11] o si se utiliza firma electrónica longeva [12].

Empresas de algunos sectores, por ejemplo las que elaboran contenidos digitales o las del sector sanitario, conservan documentos que han elaborado bien por sus características singulares, documentos digitalizados, historias médicas, bien porque es posible su posterior difusión o la creación de obras derivadas en el futuro a partir de ellas, por ejemplo: obras de arte, fotografías, videos.

Para conservar los documentos más allá del tiempo en el que se está trabajando con ellos hay que tener en cuenta:

- El posible **envejecimiento y deterioro físico** del soporte ya que los soportes magnéticos, fotográficos o el papel necesitan condiciones ambientales específicas para su conservación (humedad, temperatura, aislamiento,…). Y aún en las condiciones ideales las cintas magnéticas pueden durar en torno a 25 años si bien depende del número de reproducciones. Los discos ópticos, según los fabricantes podrían durar hasta 50 años. En cambio los discos duros se deteriorarán antes de 10 años, con un tiempo medio entre fallos de 2 a 9 años. Para las memorias electrónicas la duración es aún menor, de unos 10 años.

- La **obsolescencia** del formato y del software o del hardware para reproducirlo: interfaces que dejan de usarse y no se encuentran en el mercado, sistemas operativos que han evolucionado sin compatibilidad hacia atrás, programas ad-hoc, etc.

Para preservar los documentos electrónicos a largo plazo se pueden emplear una variedad de técnicas:

- Refresco, es decir realizar copias de los originales antes de que los soportes se deterioren, pueden realizarse en el mismo tipo de soporte o en otro que tenga mayor duración.

- Conservar el entorno tecnológico para reproducirlos, hardware, software, sistemas operativos, aplicaciones… realizando un mantenimiento periódico.

- Emular o recrear el entorno con equipos y software más actuales que permitan su reproducción.

- Migrar los equipos, programas y formatos a otros más actuales.

6 Políticas

Para poder mantener de un modo seguro y eficaz todos estos sistemas de información es importante que la empresa especifique cuáles son las reglas, criterios y procedimientos que deben seguir todos los usuarios de los sistemas para:

- Que se garantice el acceso de los recursos de información por los usuarios o programas autorizados
- Evitar la fuga de información
- Evitar el deterioro de la información almacenada o que deba ser conservada
- Evitar el uso de dispositivos no autorizados
- Proveer métodos de recuperación de la información y la actividad en caso de fallos técnicos, accidentes o desastres
- Garantizar que al terminar su vida útil los soportes son desechados correctamente (que se tratará en otra guía)
- Conocer cómo tratar las incidencias, las fugas de información y los desastres u otras contingencias [13]

Así, se identifican relacionadas con el almacenamiento las siguientes políticas necesarias en la empresa, para que sean conocidas por los propios usuarios y controladas por los responsables:

- Política de almacenamiento local en los equipos de trabajo
- Política de almacenamiento en la red corporativa
- Política sobre el uso de dispositivos externos
- Política de almacenamiento en *cloud*
- Política de copias de seguridad

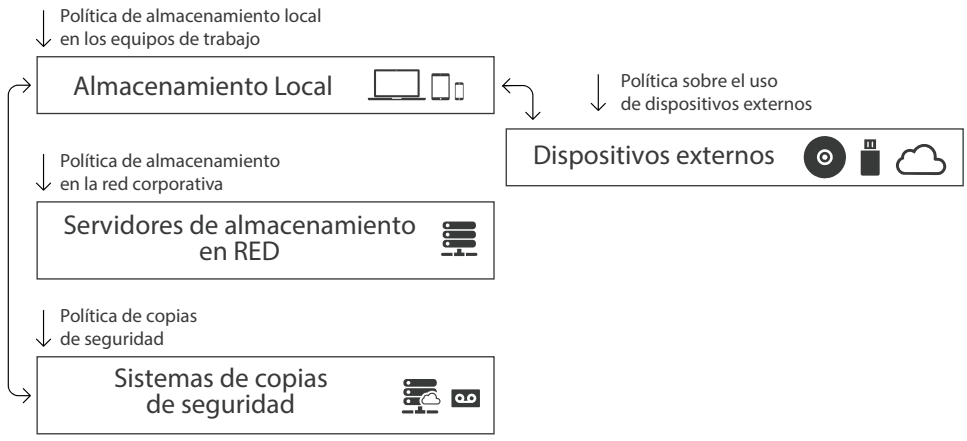


Ilustración 6: Políticas de almacenamiento en los entornos empresariales

«La empresa debe establecer unas normas de almacenamiento para los equipos de trabajo»

Otras políticas necesarias para la buena gestión de la información en la organización son:

- Política de conservación o archivo de documentos
- Política para el uso de dispositivos móviles personales o BYOD

6.1 Políticas de almacenamiento local en los equipos de trabajo

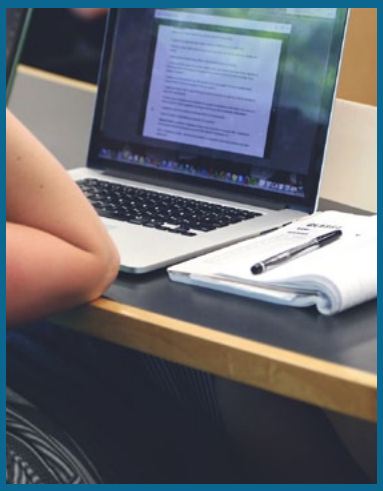
En primer lugar, la empresa establece unas normas de almacenamiento para los equipos de trabajo (equipos de sobremesa, equipos portátiles, teléfonos y otros dispositivos) que los usuarios deben cumplir. Esta política incluye al menos los siguientes aspectos:

- Qué tipo de información se puede almacenar en los equipos locales
- Cuánto tiempo debe permanecer dicha información en los mismos
- Permanencia de la información en la red local una vez transmitida a los servidores corporativos
- Ubicación dentro del árbol de directorios del equipo
- Utilización de sistemas de cifrado de información en los documentos empresariales
- Normativa para los empleados relativa al almacenamiento de documentos personales, archivos de música, fotografías, etc., y en concreto relativa a archivos que estén bajo algún tipo de regulación en cuanto a derechos de autor (descargas desde los equipos de trabajo)

6.2 Políticas de almacenamiento en la red corporativa

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa. Estas políticas explican:

- Los servidores de almacenamiento disponibles en la red corporativa están configurados para poder almacenar y compartir aquella información de la empresa que deba ser utilizada por los empleados.
- Los controles de acceso son definidos por la dirección y el responsable de sistemas, con el objetivo de definir quién puede acceder y a dónde.



«Es importante concienciar al empleado que la información almacenada en la red corporativa debe ser relevante para el trabajo»

El contenido de la información almacenada se determina a través de una política de uso específica que debe cubrir al menos los siguientes aspectos:

- Tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema
- Personas encargadas de la actualización de dicha información en caso de modificación

Los empleados pueden disponer de buzones o carpetas personales dentro de la misma red corporativa. En estas carpetas se almacena información que, si bien tiene relación con su trabajo, no necesariamente es compartida por otros miembros del equipo. Para controlar dicha información, se deben especificar políticas que incluyan los mismos aspectos que los relacionados con el almacenamiento local.

Es importante concienciar al empleado que toda aquella información almacenada en estos espacios debe ser relevante para el trabajo. La información carente de valor se elimina una vez que se haya utilizado. Así se evita que la capacidad de almacenamiento se vea desbordada innecesariamente.

6.3 Políticas sobre el uso de dispositivos externos conectados

Especialmente importante son las normas relativas al uso de equipos externos, -conocido como BYOD *(Bring Your Own Device)*- que, conectados directamente a los equipos de trabajo, permiten el almacenamiento extra de información con el objeto de trasportarla a otra ubicación o simplemente disponer de una copia de seguridad personal.

Esta política incluye al menos los siguientes aspectos:

Si está permitido o no el uso de estos dispositivos

En caso afirmativo, qué tipo de información en ningún caso está permitido almacenar, como aquella que contiene datos personales de clientes, etc.

Qué medidas de borrado se han de utilizar cuando esta información deja de ser necesaria

6.4 Políticas de almacenamiento en la nube

En el caso de que la empresa ponga a disposición de los empleados algún tipo de almacenamiento *cloud* (en la nube), esta política debe incluir al menos los siguientes aspectos:

«Una copia de seguridad es un duplicado de ficheros o aplicaciones con la finalidad de recuperar los datos en caso de daños o pérdidas del sistema»

- Si está permitido o no el uso de servicios *cloud* públicos
- En caso afirmativo, qué tipo de información en ningún caso está permitido almacenar, como aquella que contiene datos personales de clientes, etc.
- Qué medidas de borrado se han de utilizar cuando esta información deja de ser necesaria
- En los servicios *cloud* privados se establecerán los criterios para su contratación de manera que se cumplan los criterios de la organización y legales para la información que allí se almacene.

6.5 Políticas de copias de seguridad

Una copia de seguridad, también conocida como *backup,* es un duplicado que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Todo plan de contingencia [13] de una empresa requiere contar con una planificación adecuada de las copias de seguridad que se realizan, ya que la pérdida de datos puede poner en peligro la continuidad del negocio.

Algunos de los requisitos que debe cumplir la planificación de copias de seguridad son:

- Identificar los datos que requieren ser preservados. Son aquellos cuya pérdida afectaría a la continuidad del negocio.
- Establecer la frecuencia con la que se van a realizar los procesos de copia. Esta frecuencia influye en la cantidad de información que se puede perder con respecto a la fuente original. Este parámetro es de suma importancia y requiere de un análisis exhaustivo.
- Disponer el almacén físico para las copias. Este almacén se determina en función de la seguridad que requiere la información entre almacenes en el mismo edificio o remotos en edificios externos.
- Buscar una probabilidad de error mínima, asegurándose de que los datos son copiados íntegramente del original y en unos soportes fiables y en buen estado. No se deben utilizar soportes que estén cerca de cumplir su vida útil para evitar que fallen cuando vaya a recuperarse la información que contienen.
- Controlar los soportes que contienen las copias, guardándolos en un lugar seguro y restringiendo su acceso sólo a las personas autorizadas.

6

Políticas

«Cuando se deseche un soporte de almacenamiento, es importante realizar un proceso de borrado seguro»

- Planificar la restauración de las copias:
  - Formando a los técnicos encargados de realizarlas
  - Disponiendo de soportes para restaurar la copia, diferentes de los de producción
  - Estableciendo los medios para disponer de dicha copia en el menor tiempo posible
- Probar el sistema de forma exhaustiva para comprobar su correcta planificación y la eficacia de los medios dispuestos.
- Definir la vigencia de las copias, estableciendo un periodo en el que dicha copia deja de tener validez y puede sustituirse por una copia más actualizada de la información.
- Controlar la obsolescencia de los dispositivos de almacenamiento. Para el caso de aquellas copias que almacenan información histórica de la organización, por ejemplo proyectos ya cerrados, se debe tener en cuenta el tipo de dispositivo en el que se ha realizado la copia, para evitar que en el momento que se requiera la restauración de dicha información no existan ya lectores adecuados para dicho dispositivo.

Cuando se desechen los soportes de almacenamiento, porque hayan llegado al límite de vida útil fijado en la política de copias de seguridad, es importante realizar un proceso de borrado seguro o destrucción para asegurar que la información que contiene no podrá ser recuperada posteriormente.

7 Soluciones en el catálogo

El catálogo de INCIBE [14] recoge las soluciones de seguridad, productos(PR) y servicios (SR), que están disponibles en el mercado español. En el caso del **almacenamiento seguro** los **productos** están registrados fundamentalmente dentro de las categorías y subcategorías:

PR **Contingencia y continuidad:**

- **Copias de seguridad.** Son herramientas destinadas al almacenamiento de datos o información con el fin de disponer de un medio para poder recuperarlos en caso de pérdida accidental o intencionada.

- **Infraestructura de respaldo.** Son herramientas destinadas a posibilitar el despliegue rápido de infraestructura de respaldo en caso de pérdida, con el objetivo de reducir al mínimo los tiempos de interrupción de la actividad.

- **Seguridad en Virtualización.** Dentro de estas herramientas se engloban los mecanismos y tecnologías que aportan seguridad a los sistemas virtualizados.

- **Herramientas en la nube.** Son las plataformas tecnológicas que permiten configurar y utilizar recursos tanto hardware, software y comunicaciones en un tiempo mínimo para la recuperación en caso de incidente de seguridad. Se caracterizan por la transparencia para el usuario y el acceso remoto desde cualquier lugar y dispositivo.

PR **Cumplimiento legal:**

- **Herramientas de cumplimiento legal** (LOPD, LSSI, etc.). Estas herramientas permiten el cumplimiento con la legislación en materia de seguridad de la información. Se encuentra la LOPD (Ley Orgánica de Protección de Datos), LSSI (Ley de Servicios de la Sociedad de la información), LPI (Ley de Propiedad Intelectual), etc.

PR **Prevención de fuga de información:**

- **Control de contenidos confidenciales.** Son herramientas que impiden y evitan la transferencia de datos no autorizados y la fuga de información confidencial.

- **Gestión del ciclo de vida de la información** *(ILM: Information Life Cicle).* Son herramientas que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.

- **Control de dispositivos externos de almacenamiento.** Son herramientas destinadas a controlar el acceso físico de puertos y otros dispositivos extraíbles (memorias USB), para evitar el robo de información.

- **Herramientas de encriptación.** El cifrado consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean accesibles por cualquier persona que desconozca la clave de decodificación.

- **Cifrado de discos duros y soportes de almacenamiento.** Son herramientas destinadas a la encriptación de todo tipo de soportes de almacenamiento, discos duros y memorias USB.

7

Soluciones
en el catálogo

«El catálogo de INCIBE recoge las diferentes soluciones de seguridad, productos y servicios según categorías»

PR **Auditoría técnica:**

- **Auditoría de sistemas y ficheros.** Son herramientas destinadas a registrar y analizar la actividad sobre ficheros y datos de los sistemas.

- **Herramientas de recuperación de datos.** Son herramientas que recuperan rastros de un incidente que hayan podido ser eliminados de forma intencionada o accidental.

PR **Seguridad en dispositivos móviles:**

- **Seguridad para dispositivos móviles.** Son herramientas destinadas a proteger la información, como las aplicaciones y sistemas de estos dispositivos. Incorporar mecanismos de protección contra malware, copias de seguridad, protección de las comunicaciones, cifrado de los datos almacenados en el dispositivo para salvaguardar la información.

- **BYOD.** Son herramientas basadas en tecnologías de gestión de movilidad que permiten la protección de estos dispositivos. Incorporan mecanismos de autenticación accediendo a las aplicaciones y datos en cualquier dispositivo.

En cuanto a los **servicios** registrados para almacenamiento y borrado seguro se encuentran principalmente bajo las categorías de:

SR **Contingencia y continuidad:**

- **Copias de seguridad remotas *(backup)*.** Son servicios de almacenamiento de datos fuera de la organización, permitiendo la restauración de la información de forma inmediata en caso de robos o pérdida de datos.

- **Custodia y archivo seguro.** Son servicios de almacenamiento con fuertes medidas de seguridad y en un emplazamiento distante de la organización.

- **Centros de respaldo.** Son servicios diseñados de réplica y almacenamiento que permiten a las organizaciones disponer de infraestructuras secundarias ante incidentes de seguridad.

- **Gestión del ciclo de vida de la información.** Son soluciones que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.

SR **Cumplimiento legal:**

- **Adaptación a la legislación (implantación).** Son servicios destinados a llevar a cabo la adecuación de las empresas y organizaciones a la legislación aplicable, llevando a cabo la implantación de las medidas de tipo jurídico, técnico y organizativo.

- **Auditoría de legislación.** Son servicios destinados a la realización de auditorías de nivel de cumplimiento de la legislación aplicable a una empresa u organización, con el fin de determinar y analizar si la empresa ha adoptado los cambios según la legislación.

8 Bibliografía

[1] 2005, Guía INCIBE, Cómo gestionar una fuga de información: una aproximación para el empresario · https://www.incibe.es/empresas/guias/Guia_fuga_informacion

[2] BOE, LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal · http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

[3] AGPD, Portal Agencia Española de Protección de Datos · http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

[4] Guías AGPD Agencia Española de Protección de Datos · http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

[5] BOE, Colección Códigos electrónicos. Propiedad industrial · http://www.boe.es/legislacion/codigos/codigo.php?id=67&modo=1&nota=0&tab=2

[6] BOE, Colección Códigos electrónicos. Propiedad intelectual · http://www.boe.es/legislacion/codigos/codigo.php?id=87&modo=1&nota=0&tab=2

[7] Incibe - Blog - La importancia de las copias de seguridad de tus datos · https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/importancia_copias_seguridad

[8] Incibe - Blog - Razones para almacenar información corporativa en la nube · https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/razones_almacenar_informacion_corporativa_nube

[9] Incibe – Empresas - ¿Qué te interesa? - Acuerdos de Nivel de Servicio · https://www.incibe.es/empresas/que_te_interesa/Contratacion_de_servicios

[10] Incibe – Blog – Infografía ¿Borrar los datos de manera definitiva? ¡Aprende cómo! · https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/borrar_informacion_dispositivo_ciberseguridad

[11] Portal Factura- e · http://www.facturae.gob.es/paginas/Index.aspx

[12] Portal Administración electrónica – Empresas - Formatos de firma electrónica · http://firmaelectronica.gob.es/Home/Empresas/Firma-Electronica.html

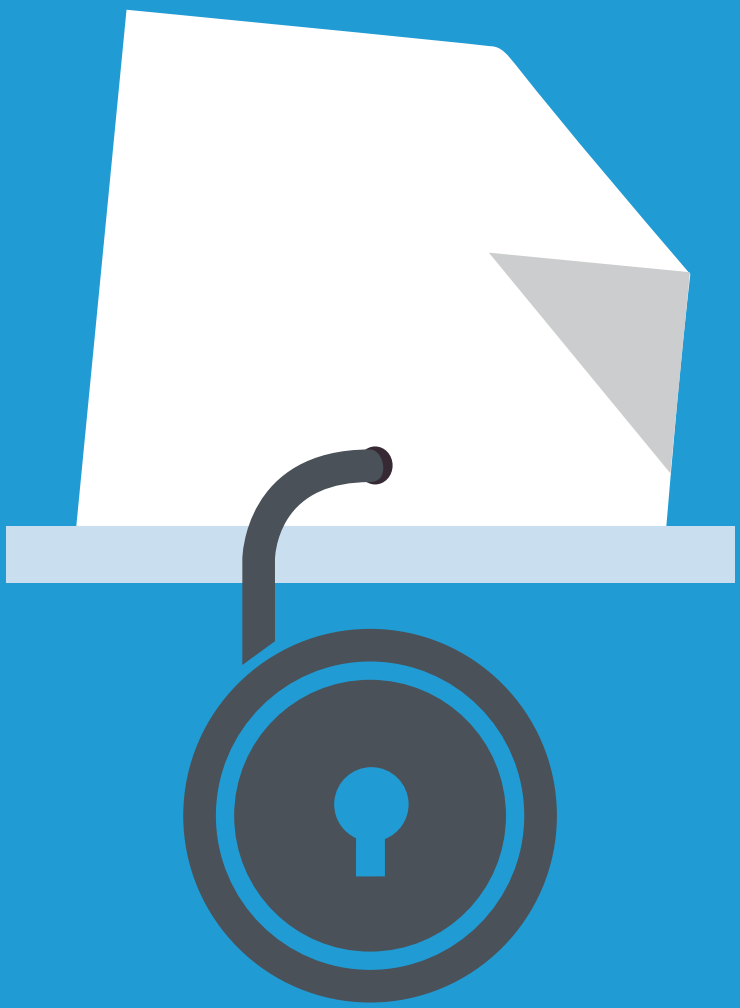
[13] Incibe – Empresas - ¿Qué te interesa? – Plan de contingencia y continuidad de negocio https://www.incibe.es/empresas/que_te_interesa/Plan_de_contingencia_y_continuidad_del_negocio/

[14] Incibe – Empresas – Catálogo · https://www.incibe.es/icdemoest/empresas/Catalogo_STIC/

[15] Incibe – Blog – Cifra tus datos, no regales la información de tu empresa · https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Cifra_datos_no_regales_informacion_empresa

[16] Incibe – Blog – Cómo proteger en 5 pasos la privacidad de la información de tu empresa desde tu puesto de trabajo · https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/proteger_cinco_pasos_privacidad_informacion_empresa_puesto_de_trabajo

[17] Incibe – Blog – La importancia de las copias de seguridad en dispositivos móviles https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/copias_seguridad_dispositivos_moviles



GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL