LA INFORMACIÓN

Un activo esencial de tu universidad
Clasificación, cifrado y metadatos
Copias de seguridad, borrado seguro y tipos de almacenamiento

UNCUYO UNIVERSIDAD NACIONAL DE CUYO
SECRETARÍA DE TRANSFORMACIÓN DIGITAL
GOBIERNO DE ESPAÑA MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
INSTITUTO NACIONAL DE CIBERSEGURIDAD SPANISH NATIONAL CYBERSECURITY INSTITUTE
metared
incibe_

ÍNDICE

1. LA IMPORTANCIA DE LA INFORMACIÓN

La información en las universidades es esencial para llevar a cabo los distintos procesos que se producen en ella: gestión académica, investigaciones, procesos administrativos, información sobre campus, etc. El almacenamiento, tratamiento y gestión de la información, en formato digital o en otros formatos son las actividades que conforman los llamados **sistemas de información** que soportan estos procesos. Estos sistemas incluyen también los datos, los recursos materiales (tradicionales, como el bolígrafo y el papel, o tecnológicos) y las personas necesarias para realizar esas actividades.

ACADÉMICAS

ADMINISTRATIVAS

INVESTIGACIÓN

DIFUSIÓN

Actividades de los sistemas de información

ALMACENAMIENTO

TRATAMIENTO

GESTIÓN

1. LA IMPORTANCIA DE LA INFORMACIÓN

La información también es un activo de la universidad:

TANGIBLE	INTANGIBLE
Ordenadores	Know-How
Dispositivos de almacenamiento	Reputación
Teléfonos móviles	Propiedad Intelectual

Si hablamos de los activos que componen estos sistemas de información, es fácil identificar, en primer lugar, aquellos más tangibles como ordenadores, dispositivos de almacenamiento, teléfonos móviles, etc. Sin embargo, no se debe olvidar que existen otros **activos de información, también esenciales para la universidad, que son intangibles** como el know-how de los docentes, estudiantes y personal administrativo, la reputación, el software, o la propiedad intelectual.

Es lógico pensar que la información es un recurso esencial para cualquier organización, más aún en aquellas que proveen servicios basados en el conocimiento, como las universidades.

Por ello, es un aspecto fundamental incidir en que **las universidades deben preocuparse por su información,** pues de no estar disponible, alterarse o difundirse sin consentimiento podría afectar a la buena marcha de la empresa. Si la información sobre nuestros procesos como institución, los datos personales y académicos de nuestros estudiantes, docentes y personal de administración, o detalles sobre proyectos de investigación cayeran en manos ajenas las consecuencias podrían ser muy negativas para nuestra actividad y nuestra reputación.

1. LA IMPORTANCIA DE LA INFORMACIÓN

A la protección de los activos de información frente a las amenazas que puedan afectar a su disponibilidad, integridad o confidencialidad la denominamos **seguridad de la información**. Los incidentes de seguridad que afectan a la información de la universidad pueden ser:

Accidentales

Los sucesos no intencionados son la causa de muchos incidentes. Algunos ejemplos son: borrado de un archivo que pensabas que ya no servía, enviar un correo a un destinatario erróneo o sencillamente una avería en el disco duro.

Intencionados por parte de miembros de la comunidad universitaria o insiders

En ocasiones son los propios miembros de la comunidad universitaria los que deciden llevarse o modificar información de la universidad, causar infecciones o facilitar el acceso a terceros. Lo hacen por motivos propios, es paradigmático el cambio de notas o sustracción de exámenes, o bajo la influencia o el soborno de ciberdelincuentes. Un insider puede causar muchos incidentes pues tiene fácil acceso a la información de la universidad. En particular, los robos o fugas de información son fáciles de realizar dado el reducido tamaño de los dispositivos de almacenamiento extraíble y su creciente capacidad, la accesibilidad a los servicios de almacenamiento en la nube o debido al acceso generalizado al correo electrónico.

Causados por ciberdelincuentes

Utilizando códigos maliciosos o malware que introducen aprovechando debilidades de nuestros sistemas y en ocasiones nuestra ingenuidad o falta de preparación, como cuando utilizan ingeniería social para conseguir el acceso esté a las órdenes de una botnet que realiza cualquier actividad delictiva.

Por tanto, es muy importante que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad que afecte a la información de tu universidad.

2. LA PRIVACIDAD Y LA LEY

La seguridad de la información consiste en conservar y proteger tres propiedades de la información:

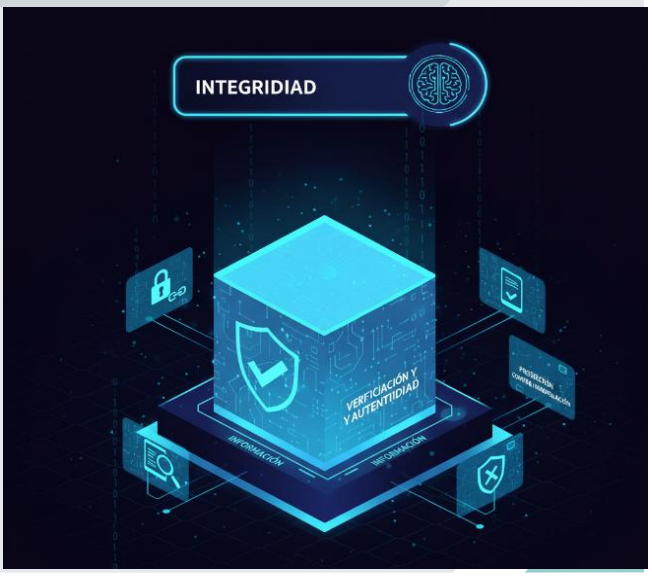
DISPONIBILIDAD - INTEGRIDAD - CONFIDENCIALIDAD

DISPONIBILIDAD

Es la propiedad que hace referencia a que la **información esté accesible cuando la necesitemos.** Por ejemplo, un fallo de disponibilidad ocurre cuando es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de ransomware, en el que los archivos son cifrados impidiéndonos el acceso a los mismos.

INTEGRIDAD

Es la característica de la **información que protegemos para que esté libre de modificaciones y errores que impliquen cambios en su contenido.** Existe un fallo de integridad cuando la información, por ejemplo, la calificación de un estudiante ha podido ser alterada intencionadamente y podemos basar nuestras decisiones en ella. Otros ejemplos de fallos de integridad son el borrado parcial, ya sea accidental o no, de bases de datos, archivos o programas.



2. LA PRIVACIDAD Y LA LEY

CONFIDENCIALIDAD

Es la propiedad por la que la **información no se pone a disposición o no se revela a individuos, entidades o procesos no autorizados,** es decir, la información confidencial es aquella que debemos proteger del acceso de personas no autorizadas. La difusión intencionada o accidental de esta información se protegerá mediante contratos de confidencialidad con usuarios o con terceros que tengan acceso a ella. A los miembros de la comunidad universitaria no les gustaría que información suya fuese expuesta sin su consentimiento y se perdería su confianza.

La información confidencial puede encontrarse en formato digital, pero también en formato físico (papel y otros soportes) o ser parte del conocimiento de las personas. Independientemente del formato en que se encuentre, se debe proteger. Es responsabilidad de los empleados conocer qué información es confidencial y a quién puede o no comunicarse. Hay distintos tipos de información confidencial:

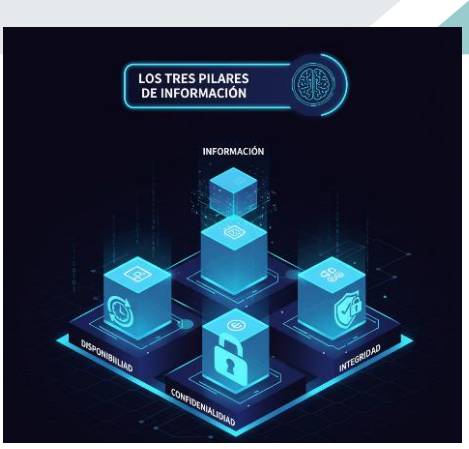
· La que es crítica para la universidad;

· La información especialmente sensible que puede interesar a otras organizaciones;

· La información protegida por la legislación como los datos personales o la propiedad intelectual;

· La que, aun no siendo datos personales, afecta a miembros de la comunidad universitaria, proveedores o socios y no debe caer en manos de terceros.

En función de los activos de información que tenga la universidad se deben seguir una serie de recomendaciones para que su seguridad sea lo más alta posible. Por ello, es importante identificarlos para los distintos procesos o los distintos servicios a los que pertenecen en un inventario de activos. A estos activos tenemos que asignarles la importancia en estas tres propiedades. Con estos datos podremos priorizar y diseñar su protección.



2. LA PRIVACIDAD Y LA LEY

Se considera **dato de carácter personal** «cualquier información concerniente a personas físicas identificadas o identificables», es decir, un DNI es un dato de carácter personal, una fotografía es un dato de carácter personal, e incluso el dato de la estatura de alguien es un dato de carácter personal, si podemos, de alguna forma, saber a quién pertenece.

La Ley exige **medidas técnicas y organizativas de seguridad** acordes al riesgo: controles de acceso, cifrado, registros de actividad, copias de seguridad, segmentación de redes, gestión de vulnerabilidades e **informes de incidentes** con acciones de contención y notificación a los titulares cuando corresponda. Los **datos sensibles** (salud, origen étnico, creencias, vida sexual, opiniones políticas o sindicales) gozan de **protección reforzada** y su uso exige base legal específica y salvaguardas adicionales.

Operativamente, UNCUYO debe: publicar **avisos de privacidad** claros en formularios y sistemas, llevar un **inventario de tratamientos** y, cuando aplique, **inscribir** las bases en el RNBD, firmar **acuerdos de encargo** con proveedores que procesen datos (incluida la localización y transferencias internacionales con protección adecuada), habilitar canales gratuitos para ejercer **derechos de acceso, rectificación/actualización, supresión y oposición**, y capacitar periódicamente a su comunidad. Este enfoque alinea la ciberseguridad institucional con la normativa argentina vigente y con las mejores prácticas recomendadas por la AAIP

Los datos personales y su privacidad se han convertido en una prioridad para la sociedad y para todas las organizaciones. Las universidades, independientemente del tamaño, deben examinar su situación en cuanto a la protección de datos personales, pues están en juego factores como la confianza de los usuarios o la competitividad.

2. LA PRIVACIDAD Y LA LEY

La privacidad y la ciberseguridad se enmarcan en normas argentinas. El eje legal es la **Ley 25.326 de Protección de los Datos Personales** y su **Decreto 1558/2001**, complementadas por disposiciones y guías de la **Agencia de Acceso a la Información Pública (AAIP)**, autoridad de control que además administra el **Registro Nacional de Bases de Datos (RNBD)**. En paralelo, el **artículo 43 de la Constitución Nacional** reconoce el **hábeas data**, garantizando a toda persona el acceso a la información propia y su rectificación, actualización o supresión.

Para UNCUYO, estos marcos implican principios y obligaciones concretas. Todo tratamiento debe ser **lícito** y, como regla, contar con **consentimiento libre, previo, expreso e informado**; existen excepciones cuando el tratamiento se vincula con **competencias propias de la administración pública**, el cumplimiento de obligaciones legales o la ejecución de contratos. Los datos se recolectan con **fines determinados y legítimos** y solo en la **medida necesaria** (minimización); deben ser **exactos y actualizados**, y **suprimirse o bloquearse** cuando dejen de ser necesarios.

Si realiza tratamientos de alto riesgo, con datos especialmente protegidos o a gran escala

- Si se considera que no son tratamientos de alto riesgo, se debe justificar la decisión.

La universidad debe garantizar la confidencialidad, integridad y disponibilidad de los tratamientos y datos personales.

La universidad debe permitir que las autoridades puedan verificar que el tratamiento de datos se realiza de forma correcta a su nivel.

La universidad debe garantizar los derechos y libertades de los afectados

- Aviso de privacidad en formularios y sistemas (finalidad + derechos + contacto).
- Mapa de bases de datos y ver si alguna debe inscribirse en el RNBD.
- Política y controles de seguridad según Res. 47/2018 (capacitación incluida).
- Contratos con proveedores con cláusulas de privacidad/seguridad y, si hay nube exterior, cláusulas modelo 2023.

3. CLASIFICACIÓN DE LA INFORMACIÓN

Bases de datos, hojas de cálculo, facturas, datos personales de estudiantes, etc., son muchos los datos que gestiona una universidad y no todos tienen la misma criticidad. Una de las partes más importantes a la hora de proteger la información de una universidad es clasificarla correctamente antes de tomar ninguna acción. El proceso de clasificación SE puede dividir en 4 pasos.

- Inventariado de los activos

  Etapa fundamental en la que **se deben tener en cuenta todos los recursos con los que cuenta la universidad, tanto en formato físico, como en formato digital.** Además, es conveniente catalogar otras características de los activos como su tamaño, ubicación o departamentos que intervienen en su gestión.

- Criterios declasificación

  La universidad debe escoger los criterios que mejor se adapten a sus circunstancias. Estos pueden ser las necesidades o requisitos de confidencialidad, integridad y disponibilidad de cada activo para las actividades principales de la misma. Un ejemplo orientativo sobre cómo clasificarla en base a la confidencialidad de esta sería:

Confidencial
información de gran relevancia para el futuro de la universidad;

Restringida
accesible, únicamente, para determinado personal de la universidad y sin la cual no pueden desempeñar su trabajo;

Uso interno
accesible, exclusivamente, para el personal de la universidad;

Pública
información de dominio público como, por ejemplo, la publicada en la página web.

- Clasificar cada activo.

El siguiente paso consiste en **etiquetar cada activo** de forma adecuada, un ejemplo sería añadiendo etiquetas al comienzo del nombre del archivo.

[confidencial]Proyectos_2020.docx
[restringido]nóminas_2018.xlsx
[interno]Cuadrantes_mes.xlsx
[publico]Historico_mensajes_Redes_Sociales.xlsx

También podrían utilizarse marcas de agua o códigos de color.

- Tratamiento de la información

El siguiente paso consiste en elaborar un listado con los controles de seguridad que se llevarán cabo para proteger cada activo. Un ejemplo del tratamiento que recibirá cada tipo de información, en función de su confidencialidad, será:

LIMITAR EL ACCESO – CIFRADO – COPIAS DE SEGURIDAD – CONTROLES ESPECIFICOS – ACUERDOS DE CONFIDENCIALIDAD

Limitar el acceso de personas o grupos. Se deberá llevar un control de accesos para que la información sea accesible, únicamente, por el personal que la necesite para su trabajo, según los roles o perfiles. Por ejemplo, los datos de estudiantes no son necesarios para el personal de RRHH. No toda la Comunidad Universitaria debe tener acceso a todos los recursos.

3. CLASIFICACIÓN DE LA INFORMACIÓN

A la hora de proteger la información en formato electrónico, una de las medidas más eficaces es el cifrado de la información. Mediante esta técnica podemos **ofuscar cualquier fichero y hacerlo inaccesible a otras personas que no sepan la clave de descifrado.**

El cifrado es una de las mejores medidas de seguridad para el almacenamiento y transmisión de **información sensible, especialmente a través de soportes y dispositivos móviles o servicios de almacenamiento en la nube.**

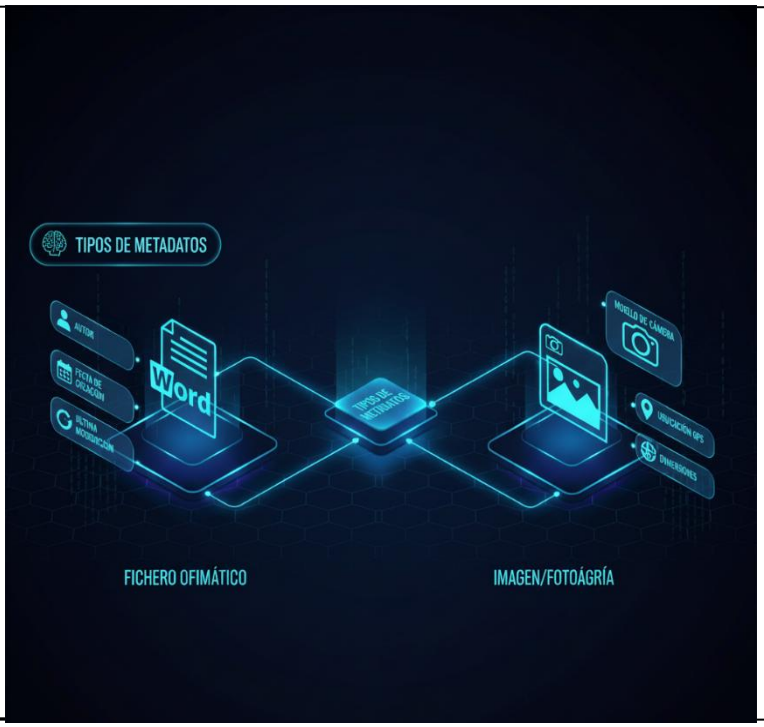
- Cifrado
- Copias de Seguridad
- Medidas específicas como las indicadas en el primer parte del documento.
- Medidas específicas para la información sujeta a acuerdos de confidencialidad.

¿QUE ES UN METADATO?

Un **«metadato»** es aquella información que incluye ficheros digitales pero que no forma parte del contenido. Algunos ejemplos de metadatos son la fecha de creación, la fecha de modificación o el autor del fichero.

3. CLASIFICACIÓN DE LA INFORMACIÓN

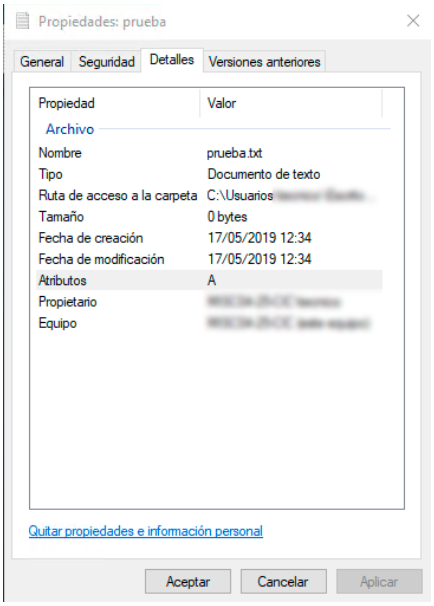
Debemos tener en cuenta que cada tipo de fichero tiene sus propios metadatos. Por ejemplo, mientras que un fichero ofimático como un Word puede contener el autor del documento, una imagen puede incluir además sus dimensiones, información de dónde se tomó la foto o incluso el modelo de cámara utilizado.



Aunque pueden ser muy útiles, **en algunos casos pueden proporcionar información valiosa sobre nosotros a los ciberdelincuentes como** nombres de usuario, fechas de creación o modificación de los documentos, ubicación de las fotografías, aplicación utilizada, etc.

Por ello, debemos eliminar los metadatos antes de enviar el fichero a otra persona, o subirlos a la página web de la universidad o a un servicio de almacenamiento en la nube.

La mayoría de los programas de ofimática más utilizados incorporan funcionalidades para eliminar esta información. También se puede hacer desde el propio sistema operativo como es el caso de Windows mediante la opción de botón derecho -> Propiedades -> Detalles. A continuación, se selecciona «Quitar propiedades e información personal» y se abrirá una nueva ventana. Se selecciona la opción «Quitar las siguientes propiedades de este archivo» y posteriormente «Seleccionar todo». Por último, clic en «Aceptar» y el proceso de borrado de metadatos ha terminado.



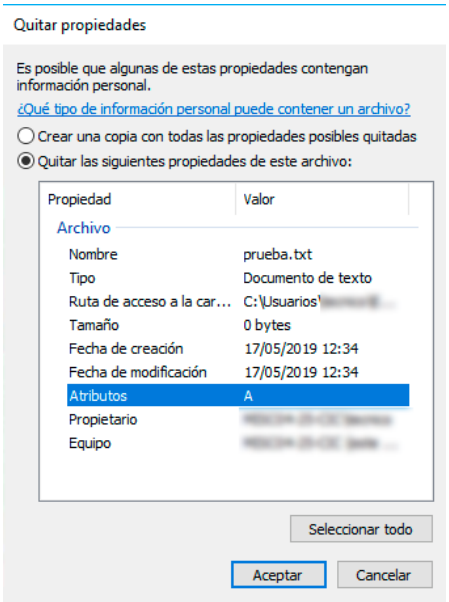


Ilustración 1. Los tres pilares de la seguridad de la información

Ilustración 2. Pasos para borrar los metadatos mediante *Windows 2*

4. COPIAS DE SEGURIDAD

Una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarla**.** Desde el punto de vista institucional, ante un incidente grave o un desastre, una copia de seguridad puede marcar la diferencia entre recuperarse o sufrir las consecuencias, en ocasiones tan severas que pondrán en riesgo su continuidad.

Cualquier universidad debe contar con un sistema de copias de seguridad que proteja su información ya que en muchos casos esta es la única garantía de poder continuar con la actividad institucional.

1. ¿Qué información copiar?

El primer paso, será **determinar la información que se debe copiar**. Para ello, como ya explicamos en el apartado primero del tema anterior, **se tiene que clasificar.** En función de esa clasificación se identificarán aquellos activos de información sin los cuales la empresa no podría seguir con su actividad diaria.

2. ¿Cada cuánto tiempo se debe realizar la copia de seguridad?

Determinar la periodicidad con la que se harán las copias de seguridad dependerá de cada empresa en particular. Se ha de definir **una frecuencia adecuada para que, ante un problema con cualquier activo de información, no suponga una gran pérdida y no afecte negativamente a la actividad laboral.**

3. ¿Dónde almacenar la copia de seguridad?

El tipo de soporte a elegir para almacenar las copias de seguridad dependerá de varios factores como la cantidad de información a copiar, del sistema seleccionado y la inversión a realizar. Las ventajas e inconvenientes de los tipos de almacenamiento más comunes son:

- **Cintas magnéticas:** la principal ventaja de este medio de almacenamiento es su reducido coste para almacenar grandes cantidades de datos. Diferentes estudios demuestran que el auge de esta tecnología como medio de almacenamiento para las copias de seguridad se debe a que se considera más fiable que los discos duros, además de poseer una vida útil superior a 30 años y un menor coste por terabyte.

- **Discos duros externos:** este tipo de soportes presentan varias ventajas como la facilidad de configuración o mejores tasas de rendimiento respecto a las cintas magnéticas. Por el contrario, presentan una vida útil inferior y un mayor coste por terabyte que las cintas. En empresas cuyo volumen de datos es reducido puede ser la opción más conveniente.

- **Dispositivos NAS o Network Attached Storage:** este tipo de dispositivos de almacenamiento se han diseñado, específicamente, para almacenar información. Su coste varía en función del número y tipo de discos empleados, además la gestión de las copias se simplifica al utilizar, únicamente, un dispositivo central. La mayoría de los fabricantes de estos dispositivos disponen de aplicaciones de copia de seguridad.

- **Servicios de almacenamiento en la nube:** este tipo de almacenamiento consiste en salvaguardar las copias de seguridad en servidores de terceros. La única preocupación será exigir las garantías de seguridad pertinentes a la empresa que se encargue de facilitar dicho servicio. Las ventajas de utilizar la nube como sistema de copias de seguridad son varias.

  - copia de seguridad fuera de la empresa;
  - disponibilidad de los datos en cualquier momento.
  - copia protegida ante incidentes dentro de la empresa.

  Pero también presenta desventajas, siendo las dos principales la **pérdida de confidencialidad y la dependencia de la conexión a Internet.** Como en cualquier copia de seguridad que se aloja fuera de la oficina, es recomendable cifrarla antes de subirla a la nube.

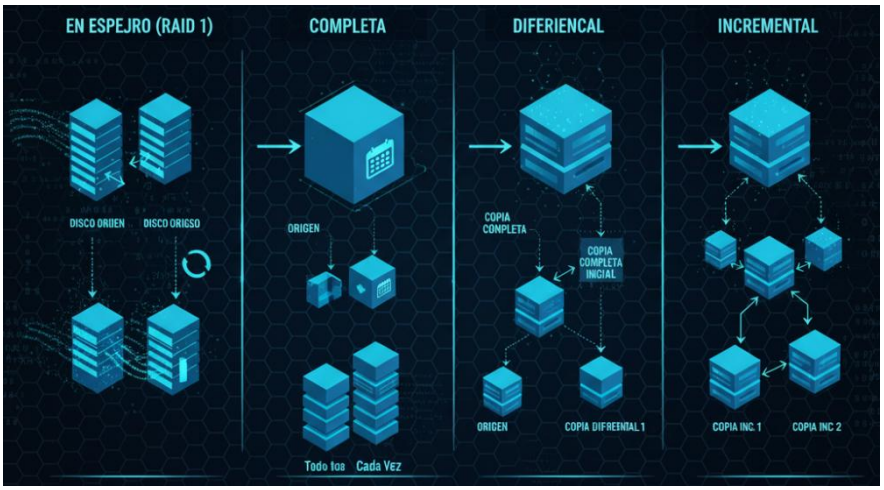
- **Discos ópticos:** la utilización de Blu-ray como dispositivos de almacenamiento está ganando popularidad en empresas que no necesitan una gran capacidad de almacenamiento, ni hacer copias de seguridad muy frecuentemente. Uno de sus mayores atractivos es la protección que ofrece ante posibles ataques de tipo ransomware dirigidos a las copias de seguridad, ya que permanece en un soporte generalmente no conectado y además suelen ser de una sola escritura. Por otra parte, su coste es muy ajustado.

4. ¿Qué tipo de copia elegir?

El siguiente paso será establecer la estrategia a seguir en cuanto a cómo realizar la copia de seguridad. Existen, principalmente, cuatro formas de realizar las copias de seguridad:

- **En espejo o RAID 1:** mediante este método se crea una copia exacta de los datos en tiempo real, mientras se trabaja, se crea una copia espejo de la información en otra ubicación. Sus ventajas son:
  - » copia realizada en tiempo real;
  - » la recuperación es un proceso muy ágil;
  - » se optimiza el espacio de almacenamiento, ya que no se guarda información antigua o en desuso.
    - Su principal desventaja es que ante borrados, modificaciones o infecciones por malware ambos discos se verían afectados.
- **Completa:** consiste en hacer una copia de todos los datos de nuestro sistema en otro soporte haciendo que la recuperación, en caso de incidente, sea mucho más rápida. Pero este método también presenta desventajas:
  - » Requiere una mayor capacidad de espacio;
  - » Mayor tiempo en realizar la copia;
  - » Mayor coste debido a la necesidad de más espacio de almacenamiento.
- **Diferencial:** únicamente se copian los archivos y directorios que han sido creados o modificados desde la última copia completa. Sus principales ventajas son:
  - » No requiere tanto espacio como la completa;
  - » La restauración de la copia es un proceso bastante simple; Aunque también presenta desventajas.
  - » No es la solución más optimizada en cuanto a tiempo y espacio utilizado.

- **Incremental:** solo se copiarán los datos que hayan variado desde la última copia de respaldo realizada, ya fuera incremental, diferencial o completa. Sus principales ventajas son:
  - » Su principal ventaja es que se necesita un espacio y tiempo menores que en las otras opciones. La restauración de la copia es un proceso bastante simple.
  - » Por el contrario, su principal desventaja es la restauración, ya que esta puede resultar mucho más compleja.



5. La estrategia3-2-1

Una buena práctica a la hora de realizar copias de seguridad es adoptar **la estrategia 3-2-1 que se basa en diversificar las copias de seguridad.** Sus claves de actuación son:

- 3: mantener 3 copias de cualquier fichero importante: el archivo original y 2 backups;
- 2: almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos.
- 1: almacenar 1 copia de seguridad fuera de nuestra empresa, lo que también se conoce como backup offsite. La copia de seguridad en la nube es un claro ejemplo de este tipo de copia.

5. BORRADO SEGURO DE LA INFORMACIÓN

¿Qué ocurre cuando la información deja de ser necesaria o útil para la empresa? Una vez llega a la última fase de su ciclo de vida, será necesario destruirla, de forma segura, de tal manera que no vuelva a ser accesible.

Existen muchos tipos de datos, contables, fiscales, de videovigilancia, etc., y todos ellos presentan una vida útil distinta. Cuando estos datos dejen de ser necesarios para la organización deben eliminarse y se debe garantizar que la información no vuelva a ser accesible para nadie. Cuando la destrucción de la información no se realiza correctamente se expone a la empresa a sanciones legales y a posibles daños de imagen, además de aumentar el riesgo a que se produzca una fuga de información.
En los casos en que el dispositivo de almacenamiento ya sea un ordenador, un smartphone o cualquier otro, sea retirado de los activos empresariales por el motivo que sea, también debe de pasar por el proceso de eliminación, de forma segura, de toda la información que contenga.

El primer paso será realizar un inventariado de activos para que ninguno sea extraviado. Se deben inventariar **todos los dispositivos y soportes que permitan el almacenamiento** como DVD, memorias USB, discos duros, ordenadores o smartphones. También se debe tener bajo control la información en formato físico.

5. BORRADO SEGURO DE LA INFORMACIÓN

El siguiente paso será eliminar la información:

- Para la información **en soportes no electrónicos como papel y soportes magnéticos** como los DVD o cintas magnéticas, se deberá utilizar el triturado como modo seguro de eliminación.
- **Los dispositivos de almacenamiento que permitan su reutilización deben ser sobrescritos múltiples veces** para evitar que la información vuelva a ser accesible.
- Los **teléfonos móviles** que se vayan a reutilizar se cifrarán antes de borrarlos y se restaurarán a sus valores de fábrica.
- **Los soportes de almacenamiento electrónico que no funcionen** o se hayan quedado obsoletos, se deberán borrar por medio de **desmagnetización o destrucción física.**
- Habrá que prestar **especial atención a los dispositivos móviles, así como a la memoria SD** que tienen algunos modelos en el momento de deshacernos de los mismos, ya que podrían contener información importante o confidencial.

Será importante hacer uso de herramientas que permitan documentar todas las operaciones de borrado.

También existe la posibilidad de hacer uso de la **destrucción certificada.** Este tipo de borrado se realiza a través de una empresa que llevará a cabo los procesos de eliminación de la información, garantizando tanto la gestión, como el control de recogida, transporte y destrucción del material. Posteriormente, estas empresas emitirán un certificado que garantizará y legitimará la validez del proceso.

6. ALMACENAMIENTO LOCAL, EN RED O EN LA NUBE

Almacenar la información usada en el día a día de la empresa, en el lugar adecuado, es importante, ya que de esta manera todos los activos estarán protegidos.

Supongamos que se guardan ciertos documentos importantes en el almacenamiento local de tu equipo por comodidad cuando se supone que deberían estar en un servidor interno. Si el ordenador, por el motivo que fuera, se averiara, todo el trabajo hecho no valdría de nada. De igual forma, sucede si se sube a la nube información confidencial sin consentimiento y sin las medidas de seguridad adecuadas, ya que se estaría poniendo en riesgo la información y a la propia empresa.

Cada tipo de almacenamiento tiene sus pros y contras, pero se ha de seguir el criterio establecido por la organización para que ningún archivo pueda quedar sin protección:

- **Local:** almacenamiento en los propios dispositivos que es de rápido acceso y que siempre estará accesible a no ser que se produzca un fallo en el equipo. Al ser solo accesible por los usuarios de cada equipo, se producen silos no compartidos de información y de fallar el equipo, podría perderse definitivamente.
- **Red:** almacenamiento en un equipo de la red interna de la empresa que requiere de acceso a la red y permisos para poder gestionar la información. En caso de que exista esta opción en la empresa, será la que debamos utilizar, ya que así toda la información estará centralizada y se podrán aplicar las medidas de seguridad de forma más eficiente.
- **Nube:** almacenamiento que siempre estará accesible si se cuenta con Internet y los permisos adecuados. Por el contrario, existe la problemática de almacenar información confidencial fuera de la empresa, por lo que habrá que utilizar herramientas de cifrado para protegerla.