¿Datos confidenciales en dispositivos obsoletos?

APRENDE CÓMO DESTRUIR
TODA
LA INFORMACIÓN
DE TUS ORDENADORES

GRUPO garatu IT SOLUTIONS

Hoy en día, en todas las organizaciones se acumula una cantidad ingente de datos, tanto en papel como, cada vez más, **en unidades digitales locales o remotas de almacenamiento**.

Esto conlleva que, más pronto que tarde, hay que entender la necesidad de mantener de forma segura la información más confidencial, tales como registros de empleados, datos financieros, contratos, información del cliente, transacciones, etc.

Tan importante es mantener esta información de forma segura durante su almacenaje, uso y acceso externo, como destruirla adecuadamente cuando no sea ya precisa, ya sea por imperativos legales, o como simple medida de seguridad.

La política de destrucción de información y su formación, **son hoy en día una parte imprescindible en la cadena de negocio**, así como una manera de, a la larga, ahorrar tiempo, equipamiento, situaciones embarazosas, y costes legales y administrativos.

De forma general, el ciclo de vida de la información consta de tres etapas:

Generación, Conservación y Destrucción.

Para ciertas pymes, resultará suficiente con eliminar los datos de soportes utilizados, ya que esos datos no resultan especialmente sensibles.

Pero muchas otras empresas que manejan datos de carácter personal y documentos confidenciales están en la obligación de **destruir eficazmente** los soportes de datos desechados.

La OMPI (Organización Mundial de la Propiedad Intelectual) establece que para que la información sea susceptible de protección esta tiene que cumplir con las siguientes particularidades:

- Tiene que ser secreta y poco accesible.
- Tener un valor comercial por ser secreta.
- Su dueño ha tenido que tomar medidas razonables para mantenerla a salvo

Por ello y para cumplir estrictamente la legalidad de la legislación vigente, cualquier empresa que trabaje con datos sensibles debe garantizar la seguridad y confidencialidad a lo largo de todo el ciclo de vida de dicha información, teniendo que establecer un protocolo que estandarice su Creación, Gestión, Archivo, Acceso y posterior Borrado.

Escoge con cuidado al receptor de la información. ¿Estás seguro de que podrá mantener la promesa de confidencialidad?

La destrucción de datos de manera eficiente no es una simple recomendación en los tiempos actuales, sino que evita sanciones por incumplimiento de la legislación.

1. Legislación Vigente

2. Solicitud del Cliente

“Derecho al olvido”

3. Política Interna

4. Seguridad

5. Obsolescencia

1. Legislación Vigente:

En muchos casos, distintas leyes obligan a las empresas a ejercer acciones de destrucción de datos en un periodo específico de tiempo.

A mediados del 2016 la LOPD fue remplazada por el más unificado a nivel europeo RGPD (Reglamento General de Protección de Datos) que es más estricto si cabe. Comenzó su aplicación el 25 de mayo de 2018.

El nuevo reglamento europeo (RGPD) advierte que **cualquier empresa que controle o procese datos tenga registros detallados de sus actividades de procesamiento.**

Además, para cumplir con el RGPD no hay que destruir únicamente los documentos en papel sino que también, hay que cumplir con una destrucción segura de discos duros, ropa laboral o falsificaciones *(en el caso de que sea necesario)*.

Por otro lado, **en ocasiones la legislación obliga a lo contrario**, mantener la información durante un número específico de años como es el caso de empresas de hospedaje, financieras, etc.

Al término de éstos, la empresa habrá de destruir esos datos de manera eficiente.

Es posible a su vez que una empresa, conscientemente o inconscientemente, haya usado material digital protegido (software, vídeo, audio, artículos, imágenes, etc.) y que sea vea obligada a su destrucción en el menor tiempo posible, o arriesgarse a recibir fuertes multas al respecto, o entrar en litigios indeseables, **dañando no sólo la economía de la empresa sino su imagen de cara al exterior**.

En muchos casos distintas leyes obligan a las empresas a ejercer acciones de destrucción de datos en un periodo específico de tiempo.

Según la RGPD son datos de carácter personal «cualquier información concerniente a personas físicas vivas identificadas o identificables».

Incluso datos que hayan sido presentados con un seudónimo, pero que pudieran utilizarse para identificar a una persona.

POR EJEMPLO:

nombres de usuarios, nombres y apellidos, direcciones postales, números de teléfono, DNI, formación, profesión, números seguridad social, correos electrónicos, firma electrónica, pruebas, diagnósticos y tratamientos médicos, rendimiento deportivo, edad, raza, afiliación política, cuentas en bancos, compras, suscripciones, visitas a páginas web, direcciones IP, uso de los servicios contratados, fotos, grabaciones de audio o videos de cámaras de seguridad, etc.

2. Solicitud del cliente “*Derecho al Olvido*”

Un cliente (individuo o negocio) en numerosas ocasiones solicita a la empresa a la que ha contratado sus servicios que destruya información existente sobre ellos y que no desean por distintos motivos que permanezca en manos ajenas.

El responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los que estén tratando tales datos personales **que supriman** todo enlace a ellos, o las copias o réplicas de tales datos.

La empresa tiene que acceder a esta solicitud de manera voluntaria **si no quiere incurrir en delito.**

Se ha de tener en cuenta **que la RGPD reconoce a las personas el derecho a que sus datos personales sean destruidos** al ser esto solicitado por el consumidor, y el no proceder adecuadamente, voluntaria o involuntariamente, puede acarrear fuertes multas.

3. Política Interna

Multitud de empresas tienen como política interna la destrucción de información al término de un proyecto o encargo.

Esta destrucción puede ser total, o parcial, eliminando la localización actual de la información y traspasándola a unidades de almacenamiento de copias de respaldo (*backup*).

Es posible a su vez que cada cierto tiempo y bajo necesidad se destruya información, ya sea por considerarse obsoleta, no teniendo valor ni sentido guardarla, o simplemente para así tener espacio para nueva información, y que ocupe el sitio de la anterior sin necesidad de invertir en nuevas unidades de almacenamiento.

4. Extremando la Seguridad:

El mantener información indefinidamente aumenta el riesgo de que tarde o temprano se filtren datos confidenciales, ya sea por un manejo interno inadecuado o por ataques exteriores que resulten en robo de información sensible.

La destrucción de información, orientada a la seguridad, ha de ser una parte esencial en la estructura de funcionamiento de una empresa.

Un simple descuido de un empleado o un proceso mal planificado puede sacar a la luz material delicado.

Tampoco hay que descartar que empleados desleales pongan en riesgo a su propia empresa, ya sea por motivos de descontento con su situación laboral, por venta de información a la competencia o para su beneficio propio.

El grupo Paradell Consultores Detectives Privados y Consultoría publicó un informe en el que se manifestaba que en el 2008 se había producido un aumento del 60% en el número de robos de información confidencial respecto al año anterior.

Los robos **estaban liderados por mandos intermedios** 27%, seguido por el **personal externo de la organización** con un 23%, los **ex trabajadores** ocupaban un 17% y el **equipo directivo** un 14%.

5. Obsolescencia

Es normal que una empresa desee modernizar sus unidades de almacenamiento al llegar éstas a su vida útil

Según va pasando el tiempo, las empresas van renovando sus unidades de almacenamiento al llegar éstas a su vida útil, o por acercarse a una edad que hace que disminuya su eficacia, siendo éstas unidades más propensas a presentar errores de lectura, escritura o fiabilidad.

Las unidades antiguas que tengan información crítica, deberán de ser destruidas según los parámetros de seguridad que se requieran.

La preservación digital, que aunque también está sujeta a la obsolescencia, al menos permite establecer mecanismos de control y prevención que favorecen la disponibilidad a largo plazo de la información.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) es la encargada de la protección de los datos de carácter personal y es muy estricta, exigiendo altos niveles de seguridad en la destrucción de documentos no sólo con soporte en papel, sino también de **plásticos, microfichas, formatos de almacenamiento ópticos (CD, CD-RW, HD DVD, VMD y Blue Ray) cintas de video, placas médicas, películas de triacetato y cualquier otro medio de almacenamiento, unidades flash USB, discos externos e internos, teléfonos móviles, PDA's, contendores multimedia, etc...**

👉 En cuanto a **destrucción de información**, el Reglamento de Protección de datos de carácter personal menciona:

«los datos personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo..»

Destrucción según tipo de soporte:

1.- Soporte papel
2.- Discos duros y removibles

1.- Soporte papel

Norma DIN 66399 para la destrucción de soporte de datos: 3 categorías de protección, 6 categorías de materiales, 7 niveles de seguridad

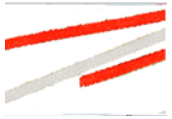
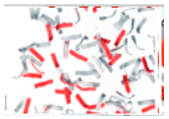
Destruir la información en papel por medio de máquinas trituradoras:

El papel tiene que hacerse desde tiras a partículas, dependiendo del nivel de seguridad que necesitan los documentos a destruir.

A mayor nivel de seguridad más pequeño debe de ser el tamaño de las tiras o las partículas. Además se estableció el sexto nivel de seguridad para usuarios especiales, que excede los
niveles de la normativa DIN estándar.

Además, si tenemos grandes volúmenes de residuos, como es el caso por ejemplo de destructoras de alta capacidad, es posible lograr un nivel de seguridad superior, tomando medidas adicionales como mezclar o compactar las tiras o partículas.

Como dato importante la nueva norma DIN 66399 fija **que si el interesado puede destruir los soportes de datos directamente en el mismo lugar donde los guardan, se incrementa la seguridad y es preferible antes que otros procedimientos externos.**

P-1	Recomendado para soportes con datos generales que han de hacerse legibles.	-Superficie **<- 2000 mm2** -Anchura de tiras **<-12mm** -Longitud tira sin determinar	
P-2	Recomendado para soportes con datos internos que han de hacerse legibles	-Superficie **<- 800 mm2** -Anchura de tiras **<-6mm** -Longitud tira sin determinar	
P-3	Recomendado para soportes con datos sensibles e información confidencial	-Superficie **<- 320 mm2** -Anchura de tiras **<-2mm** -Longitud tira sin determinar	
P-4	Recomendado para soportes con datos especialmente sensibles e infor. confidencial	-Superficie **<- 160 mm2** -Anchura de tiras **<-6mm** -Ejemplo pedazos 4x40mm	
P-5	Recomendado para soportes con datos e información secretos	-Superficie **<- 30 mm2** -Anchura de tiras **<-2mm** -Ejemplo pedazos 2x15mm	
P-6	Recomendado para soportes con datos secretos con precauciones de alta seguridad	-Superficie **<- 10 mm2** -Anchura de tiras **<-1mm** -Ejemplo pedazos 0,8x12mm	
P-7	Recomendado para soportes con datos estrictamente confidenciales y máximas precauciones de seguridad	-Superficie **<- 5 mm2** -Anchura de tiras **<-1mm** -Ejemplo pedazos 0,8x5mm	

2.- Discos duros y removibles

Todo el mundo sabe que un simple borrado de los datos no es suficiente para eliminarlos totalmente, pero todavía muchos creen que un formateado del disco impedirá su recuperación.

Nada más lejos de la realidad, ya que **existen simples herramientas que permiten recuperar ficheros de un disco formateado** con excelentes resultados. Por tanto, necesitamos algo que vaya más allá de un simple formateo.

¿Cómo pueden recuperarse los datos?

1. Utilizando herramientas específicas de recuperación de datos se puede recuperar con cierta facilidad la información.
2. Existen multitud de herramientas freeware para la recuperación de datos: Autopsy, FileRecovery, etc.

Mojar un disco duro dejará inservible la parte electrónica y quizás alguna pequeña porción de datos, pero para una empresa especializada es fácil recuperar la información.

2.- Discos duros y removibles

Los métodos más eficaces para la destrucción de la información contenida en nuestros dispositivos de almacenamiento son **la destrucción física, la desmagnetización y la sobreescritura.**

LA DESTRUCCIÓN FÍSICA

Este método no da la posibilidad de recuperación.
Válido para la destrucción de dispositivos no regrabables, ópticos y magnéticos. Suele llevarse a cabo en destructoras de metal o en alguna planta de incineración que haya sido validada de antemano para realizar estas operaciones de manera segura y eficaz. También se puede hacer de una manera casera, casi al 100% efectiva o en su defecto con unos costos demasiados elevados de recuperación, como para que alguien decida hacerlo.

LA DESMAGNETIZACIÓN

Este método no da la posibilidad de recuperación.
Únicamente válido para dispositivos de almacenamiento magnético. Es la exposición de los soportes de almacenamiento a un campo magnético. Cada dispositivo necesita de una potencia específica para asegurar la completa polarización de todas sus partículas.

LA SOBREESCRITURA

Te da la posibilidad de recuperar el dispositivo para volver a reutilizarlo con todas las garantías. Consiste en la escritura de un patrón de datos sobre la información que está en los dispositivos de almacenamiento.

Meter en un microondas los CD, DVD, magneto ópticos para ser destruidos puede ser peligroso y dañar permanentemente el horno

Diferentes métodos de sobreescritura

Método de borrado	Definición	Nivél de Seguridad
Grado1 – Superfast Zero Write	Sobreescritura del dispositivo con un valor fijo (0x00) en cada tercer sector.	**Bajo**
Grado2 – Fast Zero Write	Sobreescritura del dispositivo con un valor fijo (0x00) en cada tercer sector.	**Bajo**
Grado3 –Zero Write	Sobreescritura del dispositivo con un valor fijo (0x00) en todo el área al completo.	**Bajo**
Grado4 – Random Write	Sobreescritura del dispositivo con valores aleatorios. Su fiabilidad aumenta con el número de pasadas.	**Medio**
Grado5 – Random & Zero Write	Después de sobreescribir el dispositivo con valores aleatorios, se vuelve a sobreescribir de nuevo con un valor fijo (0x00), vuelve a sobreescribir con valores aleatorios y termina con escritura de valor 0.	**Medio**
Grado6 – US Navy, NAVSO P-5239-26 MFM	Estándar de la Armada de USA NAVSO P-5239-26 para discos codificados con MFM (Modified Frequency Modulation) Consiste en la escritura de un valor fijo (0xfffff) sobre el soporte, después de un valor fijo (0xbfffff) y finalmente una serie de valores aleatorios. El área de datos se lee para verificar la sobreescritura. Suele ser aplicado sobre disquetes.	**Medio**
Grado7 – US Navy, NAVSO P-5239-26 RLL	Estándar de la Armada de USA NAVSO P-5239-26 para discos codificados con RLL (Run Length Limited) Este método aplica la escritura de un valor fijo (0xfffff) sobre el soporte grabado, un valor fijo (0x27fffff) y finaliza con valores aleatorios. El área de datos se lee para verificar la sobreescritura. Es aplicable a discos duros y soportes ópticos como el CD, DVD o el disco BlueRay.	**Medio**
Grado8 – Bit Toggle	Sobreescritura de toda la zona de datos cuatro veces. El primero con valor (0x00), sigue con el valor (0xff), después (0x00) finalizando con (0xff)	**Medio**
Grado9 – Random RandomZero	Sobreescritura del soporte dos veces con valores aleatorios y una vez más con valor fijo (0x00) Y volver a repetir el proceso nuevamente. Este método es más seguro que Random&Zero Write.	**Medio**
Grado10 – US Department of Defense (DoD 5220,22-M)	Fue introducido por el Pentágono y es conocido como “DoD 5220,22-M”. Consiste en la sobreescritura del soporte con un valor fijo determinado una vez (0x00) seguidamente se escribe su valor complementario (0xff). Finalmente se repasa con valores aleatorios. El disco se verifica para comprobar la escritura correcta de los valores.	**Medio**
Grado11 – US Air Force, AFSSI5020	Sobreescribe el soporte con un valor fijo (0x00) después otro valor fijo (0xff). Finalmente con valor aleatorio constante. Se comprueba al menos un 10% del disco para verificar la sobreescritura.	**Medio**
Grado12 – North Atlantic Treaty Organization - NATO	Estándar de borrado de la OTAN. Sobreescribe el soporte 7 veces. Las primeras 6 son de sobreescritura con valores fijos alternativos entre cada pasada (0x00) y (0xff). La séptima pasada sobreescribe con valor aleatorio	**Alto**
Grado13 – Peter Gutmann Secure Deletion	Creado por Peter Gutman en 1996. Se sobreescribe grabando valores aleatorios 4 veces sobre cada sector. Seguidamente se sobreescribirá todo el soporte con valores pseudoaleatorios sobre cada sector durante 27 pasadas, terminando con valores aleatorios durante 4 pasadas sobre cada sector. En total se realizan 35 pasadas.	**Alto**
Grado14 – US Department of Defense (DoD 5220,22-M + Gutmann Method)	35 pasadas complementables con iteracciones de Mersenne. Combina el Grado 13 y el 10.	**Muy Alto**

¿Y qué decir de las unidades de estado sólido (SSD) o memoria de flash?

En los discos tradicionales los datos se guardan en platos cubiertos por una película magnética, y que mediante un brazo mecánico con cabeza escritora/lectora se guarda/accede a información magnéticamente.

Los SSD (incluido memorias USB y tarjetas de memoria) sustituyen la mecánica por electrónica y el magnetismo por chips de almacenamiento.

En una unidad SSD **mojar su electrónica** puede hacer imposible volver a recuperar la información almacenada.

Así mismo la desmagnetización puede servir, pero habrá que utilizar imanes extremadamente potentes.
Os aconsejamos abrir el disco duro, dejar los platos al aire y entonces utilizar el imán.

Con estás dos opciones, el disco estará irrecuperable, **pero no podremos asegurar al 100% la posibilidad de recuperar la información.**

La forma más eficiente de destruir toda la información de una unidad SSD es quemarlo en una incineradora profesional.

**Un martillo puede servirte para las unidades SSD o memoria de flash.
Al golpearlo con que se destroce una sola de sus celdas de memoria, sería imposible su recuperación**

Destrucción física

La destrucción física del disco duro es **la manera más efectiva** de que los datos desaparezcan para siempre, pero evidentemente **el disco queda inoperable**.

Existen empresas destructoras especializadas que extienden un certificado donde aseguran la eliminación total.

Pero la destrucción física es algo que podríamos realizar por nosotros mismos sabiendo los pasos a dar:

Separar primero la parte electrónica de la física y dejar el plato a la vista. Golpear el plato con un martillo hasta romperlo. Es mejor realizar esta acción cuando está girando.

Lijar toda la superficie del plato con una lija potente es otro de los métodos seguros para dañar el dispositivo.

Taladrar el disco por completo también lo deja inutilizable

Con estas practicas, o la combinación de ellas, la eliminación será un éxito.

Y si después se quema, ¡mejor que mejor!

Tipo de destrucción más adecuada según el soporte a destruir

SOPORTE	TIPO	DESTRUCCIÓN FÍSICA	DESMAGNETIZACIÓN	SOBRE ESCRITURA
Discos Duros	Magnético	✓	✓	✓
Discos Flexibles	Magnético	✓	✓	✓
Cintas de *Backup*	Magnético	✓	✓	✓
CD	Óptico	✓	✗	✗
DVD	Óptico	✓	✗	✗
Blu-ray Disc	Óptico	✓	✗	✗
Pen Drive	Electrónico	✓	✗	✓ [3]
Discos Duros SSD	Electrónico	✓	✗	✓ [3]

Si lo que necesitas es una empresa externa que se ocupe de la destrucción de tus datos, infórmate de que sigue la norma **ISO 15713** y que emite el certificado correspondiente.

A partir de la norma **ISO 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas y que** complementa a la LOPD para la destrucción de documentos que contienen datos personales en cualquier tipo de soporte, sabemos muy bien cual es la mejor manera de garantizar la destrucción de datos confidenciales, en el caso de que nos obligáramos a ello por un contrato o acuerdo con otra empresa.

Con esta norma se definen los requisitos para la gestión y control de recogida, transporte y destrucción del material confidencial. También nos muestra a qué niveles de destrucción (nivel de triturado) según el tipo de información a eliminar y el soporte (papel, tarjetas SIM y negativos, cintas de audio y video, ordenadores, CD, DVD, microfichas...).

Cuanto más alto sea el nivel utilizado, la recuperación de la información será más difícil.

GRUPO garatu IT SOLUTIONS

info@grupogaratu.com
Tlf.: +34 943 344 645
grupogaratu.com