Destrucción de documentación confidencial

Gema Losada, Cristina Marco, Carlos Romero
Universidad Complutense de Madrid

glosada1001@gmail.com, marcodefrancisco@gmail.com, cromgom@yahoo.com

Resumen.

La actual normativa, tanto europea como española, hacen que la destrucción segura de información confidencial constituya un acto igual de importante que su almacenamiento de forma correcta y la restricción del acceso a esta, ya que de lo contrario esos datos confidenciales que han dejado de ser útiles pueden llegar a manos malintencionadas. Este trabajo, se enmarcará dentro de la legislación española, con él se pretende resaltar la importancia de la gestión de recursos que ya no van a ser utilizados, no sólo buscando el interés propio o no perjudicar a terceros, si no debido también al imperativo legal que así lo ordena. Además se mostrarán los diferentes tratamientos existentes en función de los recursos en los que estén almacenados, empresas y *software* dedicadas a estas labores. Por último antes de pasar a las conclusiones obtenidas en la realización de este documento se analizará y comentará una sentencia reciente y su correspondiente sanción por el incumplimiento de la legislación vigente.

Palabras clave:

- LOPD: Ley Orgánica de Protección de Datos.
- AEPD: Agencia Española de Protección de Datos.
- Información confidencial.

1 Contexto

La justificación de este trabajo se encuentra en la legislación sobre protección de datos, que obliga a destruir los documentos confidenciales. En este sentido existen disposiciones legales europeas, nacionales y autonómicas:

Parlamento europeo

- Decisión 1600/2002 por la que se establece el Sexto Programa de Acción Comunitario de Materia de Medio ambiente. [1]
- Directiva 95/46 /CE del parlamento europeo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. [2]

Estado español

- Real Decreto 1720/2007 por el que se aprueba el reglamento del desarrollo de la Ley Orgánica 15/1999. [3]

- Real Decreto 195/2000 por el que se establece el plazo para implantar las medidas de seguridad en los ficheros automatizados previstos en el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio. [4]
- Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. [5]
- Real Decreto 994/1999 por el que se aprueba el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. [6]
- Ley 10/1998, de residuos. [7]

Comunidad autónoma de Madrid

- Ley 8/2001 de Protección de Datos de Carácter Personal de la Comunidad de Madrid. [8]

La AEPD publicó en el 2008 una guía de protección de datos. [9]

2 Introducción

El ciclo de vida de la información consta de tres etapas: generación, conservación y destrucción. El objetivo principal de este trabajo se centra en la última fase de este proceso, en concreto la destrucción de datos confidenciales.

Debido a la importancia de esta labor a lo largo de los últimos años han sido muchos los países que han promulgado normas jurídicas sobre la protección de la documentación confidencial, aunque como ya se ha anticipado este documento se realizará dentro del marco de la legislación española.

La OMPI[1] establece que para que la información sea susceptible de protección esta debe de cumplir las siguientes características [10]:

- Ser secreta, es decir que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza ese tipo de información.
- Tener un valor comercial por ser secreta.
- Haber sido objeto de medidas razonables para mantenerla secreta, tomadas por su titular.

Atendiendo a la legislación vigente es fundamental para cualquier empresa u organización que trabaje con datos que reúnan las condiciones anteriores garantizar la seguridad y confidencialidad a lo largo de todo el ciclo de vida de dicha información; para ello se deberá establecer un protocolo que estandarice su creación, gestión,

[1] Organización Mundial de la Propiedad Intelectual

archivo, acceso y posterior borrado, independientemente del soporte utilizado para guardar la documentación.

En ese sentido, las exigencias de protección de la información personal y las necesidades de salvaguardar la reputación corporativa hacen que, la destrucción documental segura constituya una parte esencial. Por otro lado la conservación de información más allá del tiempo necesario genera costes de almacenamiento además de exponer a la empresa a riesgos de robo, uso indebido, divulgación y en suma a sanciones importantes por incumplimiento de los deberes de custodia.

La normativa española, basada en la europea, sobre protección de datos es muy estricta al respecto, exigiendo altos niveles de seguridad en la destrucción de documentos no sólo con soporte en papel, también se debe eliminar la información 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...

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. Dicho hurto estaba liderado por los 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%. La "fuga" de información se produce en un 95% de los casos en soporte digital, dejando el porcentaje restante para el papel. [15]

A la luz de estos datos se puede asegurar que un factor muy importante para la protección de documentos sensibles es el correcto control de la gestión por parte del nivel dirigente. La prudencia indica que los directivos deberán comunicar los secretos únicamente al personal que deba conocerlos; el caso más común de pérdida de información confidencial de una empresa se da cuando su personal deja de trabajar allí y pasa a otra empresa de la misma rama. También es importante que se marquen los documentos con la palabra "confidencial", si lo son, evitando la tentación de marcar todos los documentos, porque esa indicación perdería importancia y terminaría por ser ignorada. También podrán adoptarse otras medidas de precaución, como una política restrictiva de permisos de usuarios, imponer una contraseña para acceder a la información sensible, que sólo el personal autorizado saque material informático,etc.

2.1 Importancia de la destrucción

En la prensa aparecen numerosos casos de entidades que han vulnerado los derechos de sus clientes por una pésima gestión de sus archivos confidenciales, ya que, al final de su vida útil, en lugar de haber sido eliminados de forma segura han acabado siendo del dominio público; siendo estos actos punibles por la ley:

- Multa de 60.000 € a BBVA por el abandono de datos confidenciales en un descampado. [11]
- La Unidad de Investigación del Clima (UIC) de la Universidad británica de Anglia del Este denunció el robo de información y correos electrónicos que posteriormente fueron publicados. [12]

La audiencia Nacional ya ha firmado varias sentencias en las que se castiga de forma severa el incumplimiento de las normativas: LOPD y el RD 1720/2007 pudiendo imponer sanciones de hasta 60.101,21 €. [13,14]

Independientemente de la multa económica este tipo de acciones van en contra de la imagen y reputación de la organización, así como en detrimento de la confianza depositada en ella, puede implicar la pérdida de clientes o que la competencia tenga acceso a información confidencial y sensible con todos los perjuicios que esto puede acarrear.

2.2 Por qué es posible recuperar los datos

El caso del papel resulta bastante evidente que salvo que las partículas en las que se descomponga el documento sean muy pequeñas este podría ser reconstruido, por esta razón existe una normativa europea, la DIN 32757, que fija dicho tamaño en función del grado de confidencialidad.

En el caso de la tecnología digital es diferente, se han llegado a recuperar datos de discos corroídos por ácido, así que si se desea destruir físicamente el soporte se puede utilizar la misma política con respecto al tamaño de las partículas, combinada por ejemplo con la cremación, pero si se opta por una solución menos drástica que permita la reutilización del aparato es entonces cuando hay que preguntarse qué es lo que hace el sistema operativo cuando borra un fichero:

- Marca la entrada del directorio como libre.
- Marca los clúster-índice como libres.
- Marca los clústeres asociados al fichero como libres.

Nótese que en ningún momento se ha eliminado físicamente la información, simplemente se ha modificado un indicador que ahora permite que se pueda escribir encima de esos datos, cosa que antes no pasaba. Una de las aplicaciones de la informática forense es precisamente examinar y recuperar datos residuales.

Para asegurarse de que el contenido de ese fichero no podrá ser recuperado se pueden seguir los siguientes pasos:

- Marcar la entrada del directorio como libre.
- Borrar el nombre del fichero en la entrada del directorio.
- Marcar los clústeres-índices como libres.
- Marcar los clústeres asociados al fichero como libres.

- Sobreescribir el contenido de los clústeres liberados. Para hacerlo de forma segura existen diferentes métodos: por ejemplo el de Gutmann [16] que consiste en escribir sobre los datos originales una serie de 35 patrones diferentes de forma que sea extremadamente difícil obtener el contenido original.

3 Objetivos

El objetivo principal es asegurar que la confidencialidad que ha acompañado a la información durante las fases previas de su ciclo de vida se mantenga en esta última que comienza cuando se decide que ya no es útil, procediendo por tanto al borrado o destrucción de la misma.

Para poder llevar a cabo esta labor es necesario analizar la normativa interna en relación con la destrucción de información para determinar si esta es suficiente para el grado de confidencialidad a tratar y el grado de cumplimiento que se está llevando a cabo; así como revisar los procedimientos asociados a la destrucción de información para la identificación de los riesgos ligados al proceso y los controles implantados.

El alcance de dicha revisión debe comprender las diferentes tipologías de soportes: papel, informático; y adicionalmente también se deberá tener en cuenta la distribución geográfica de la entidad: dónde se ubican los CPD's[2], las oficinas, los archivos generales así como estudiar si las comunicaciones y los traslados de documentación entre ellas son seguras.

4 Proceso de destrucción

4.1 Fases:

El proceso de destrucción pasa por las siguientes fases:

1. Petición: Solicitar el servicio de destrucción de forma que se identifique de forma unívoca los soportes/información a destruir.
2. Recogida: Se recogen los soportes y se informa al solicitante que no se podrá recuperar la información.
3. Transporte y almacenamiento: En esta fase son necesarias medidas de seguridad en los procesos.
4. Destrucción: Si se requiere reutilización del soporte son necesarias herramientas de borrado, en caso contrario puede realizarse la destrucción física.

[2] Centro de Proceso de Datos

5. Confirmación: Informar al solicitante que la información almacenada en sus soportes ha sido borrada de forma segura.

La realización de estas fases depende del tipo de soporte y del nivel de confidencialidad de la información almacenada (clasificación de la información) en base a la cual puede ser necesaria una destrucción in-situ. En la medida de lo posible, debería existir trazabilidad de las acciones realizadas. Es habitual que algunas de las fases sean realizadas por proveedores externos. En este caso se debe verificar que:

- La organización ha especificado que debe efectuarse una destrucción segura de la información en el contrato.
- De acuerdo con lo que dicta la Ley Orgánica 15/1999 Protección de Datos con Carácter Personal[3] se emite un certificado de la destrucción, que especifique el método aplicado.

Para la correcta implantación de estos procesos es imprescindible un alto nivel de concienciación de los empleados de la organización para que apliquen el protocolo correspondiente de manera eficiente.

4.2 Normativa:

En una organización debe existir una normativa y procedimientos relacionados con el proceso de destrucción:

- Debe existir una clasificación de la información genérica.
- Normativa genérica que especifique como se debe tratar la información una vez deja de ser útil para la empresa.
- Procedimientos que especifiquen como se debe realizar la destrucción o borrado de la información según el soporte en el que se encuentre almacenada.

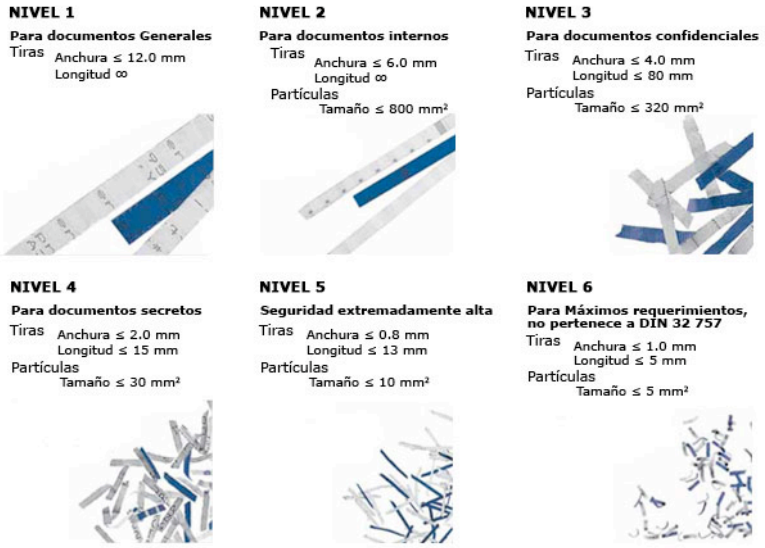
4.3 Tipo de soporte:

Hay que considerar los siguientes aspectos en relación al tipo de soporte:

- **Información en soporte papel**:

  1. Existencia de máquinas trituradoras.
  2. Comprobación del nivel de triturado aplicado según la confidencialidad del documento. Los documentos pueden ser clasificados con un nivel de seguridad según su nivel de confidencialidad. Las recomendaciones del Ministerio de Cultura para la destrucción física de documentos [17] siguen la normativa europea DIN 32757 que define cinco niveles de seguridad y aporta recomendaciones de como destruir un documento para cada una de

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



3. Importancia de la concienciación de usuarios: obligaciones y responsabilidades que tienen en relación al procedimiento.
4. Realización de pruebas de "dumpster diving[3] " para verificar que se están empleando las herramientas de triturado disponibles.

- **Información en discos duros y removibles:**
  Como se ha explicado anteriormente, el formateo normal de los sistemas operativos no reescribe toda la información del disco.

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.
3. Los soportes removibles habitualmente son considerados como consumibles.

[3] En el contexto del cibercrimen, el dumpster diving es un recurso basado en la ingeniería social. Consiste en husmear o fisgonear entre la basura para localizar notas y/o papeles de los que el usuario se ha deshecho. [18,19]

Por estos motivos es necesario aplicar un método eficiente de borrado seguro, bien sea instalando el *software* necesario para tal fin o encargando este trabajo a una empresa externa (ver ejemplos en la sección 6).

Estos son algunos de los posibles métodos de borrado a utilizar [20]:

Método de borrado	Definición	Nivel de seguridad
Grado 1. Super Fast Zero Write	Sobreescritura del soporte con un valor fijo (0x00) en cada tercer sector.	Bajo
Grad 2. Fast Zero Write	Sobreescritura del soporte con un valor fijo (0x00) en cada sector.	Bajo
Grado 3. Zero Write	Sobreescritura del soporte con un valor fijo (0x00) en todo el área al completo.	Bajo
Grado 4. Random Write	Sobreescritura del soporte con valores aleatorios. Su fiabilidad aumenta con el número de pasadas.	Medio
Grado 5. Random & Zero Write	Después de sobreescribir el soporte con valores aleatorios, se vuelve a sobreescribir de nuevo con un valor fijo (0x00), sobreescribe con valores aleatorios y termina con escritura de valor cero; este método es más seguro que Zero Write.	Medio
Grado 6. US Navy, NAVSO P-5239-26 – MFM	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con MFM (Modified Frequency Modulation). El método consiste en la escritura de un valor fijo (0xffffffff) sobre el soporte, después un valor fijo (0xbfffffff), y finalmente una serie de valores aleatorios. El área de datos se lee para verificar la sobreescritura. El método suele ser aplicado sobre disquetes.	Medio
Grado 7. US Navy, NAVSO P-5239-26 – RLL	Estándar de la Armada estadounidense (US Navy) NAVSO P-5239-26 para discos codificados con RLL (Run Length Limited). Este método aplica la escritura de un valor fijo (0xffffffff) sobre el soporte grabado, un valor fijo (0x27ffffff), y finaliza con valores aleatorios. El área de datos se lee para verificar la sobreescritura. El método es aplicable a discos duros y soportes ópticos como el CD, DVD o el disco BlueRay.	Medio
Grado 8. Bit Toggle	Sobreescritura de toda la zona de datos cuatro veces, primero con el valor (0x00), sigue con el valor (0xff), luego (0x00) y finaliza con (0xff).	Medio
Grado 9. Random Random Zero	Sobreescritura del soporte dos veces con valores aleatorios, una vez más con un valor fijo (0x00). Vuelta a sobreescribir dos veces con valores aleatorios y una última vez con ceros; el método es más seguro que Random & Zero Write.	Medio
Grado 10. US Department of Defense (DoD 5220.22-M)	Este método de borrado fue introducido por el Departamento de Defensa de los EE.UU. (Pentágono) y es conocido como "DoD5220.22-M". El método consiste en la sobreescritura del soporte con un valor fijo determinado una vez (por ejemplo 0x00), seguidamente se escribe su valor complementario (0xff) una vez, y finalmente se repasa con valores aleatorios una vez. El disco se verifica para comprobar la escritura correcta de los valores.	Medio
Grado 11. US Air Force, AFSSI5020	Estándar de las Fuerzas Aéreas de los EE.UU. (US Air Force) AFSSI5020. Este método de borrado primero sobreescribe el soporte con un valor fijo (0x00), después otro valor fijo (0xff), y finalmente un valor aleatorio constante. Se comprueba al menos un 10% del disco para verificar la sobreescritura.	Medio
Grado 12. North Atlantic Treaty Organization - NATO standard	Estándar de borrado de la OTAN (North Atlantic Treaty Organization). Sobreescribe el soporte siete veces. Las primeras seis pasadas son de sobreescritura con valores fijos alternativos entre cada pasada (0x00) y (0xff). La séptima pasada sobreescribe con un valor aleatorio.	Alto
Grado 13. Peter Gutmann Secure Deletion	El método fue creado po Peter Gutmann en 1996. Probablemente sea el método de borrado de datos más seguro que existe sin combinación con otros métodos. La sobreescritura del soporte se realiza grabando valores aleatorios cuatro veces sobre cada sector. Seguidamente se sobreescribirá todo el soporte con valores pseudoaleatorios sobre cada sector durante veintisiete pasadas. Para terminar, se escribirán valores aleatorios durante cuatro pasadas sobre cada sector. En total, se realizan treinta y cinco pasadas de sobreescritura.	Alto
Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method	Método de alta seguridad consistente en 35 pasadas, complementables con iteraciones de Mersenne, para agilizar los procesos de borrado seguro mediante la generación de números pseudoaleatorios. Combina el Grado 13 y el 10.	Muy Alto

- **Información en teléfonos móviles:**

    1. El coste de adquisición de un teléfono móvil motiva la no reutilización de estos terminales. Por lo tanto, no se exige su devolución.
    2. La mayoría de usuarios no son conscientes de que la información registrada en los teléfonos podría ser accedida por terceras personas.
    3. De los teléfonos móviles se pueden recuperar agendas, registros de llamadas, mensajes SMS y MMS.
    4. Actualmente, no existen herramientas para el borrado seguro de la información registrada en la memoria de los teléfonos móviles.
    5. La destrucción de la información se debe realizar a partir de una destrucción física de la memoria.

- **Información en PDAs:**

    1. Las PDAs disponen de procedimientos de borrado seguros (hard reset).
       No obstante, en algunos casos se ha observado que el proceso no era suficiente para las iPAQ (memoria FLASH).
    2. Se debe tener en cuenta como son tratados los equipos que, por una avería, no es posible aplicar el procedimiento de borrado.

- **Información en imágenes, videos, etc:**

    1. La LOPD[5] define la imagen como dato de carácter personal puesto que se asocia a una persona física identificada e identificable.
    2. En cuanto a la forma de obtener dicha información es necesario hacer una distinción entre aquellos dispositivos que sólo reproducen aquello que está sucediendo, y los que lo almacenan en cintas, tarjetas, etc.
    3. En el primer caso no hay ningún tipo de material susceptible de ser destruido, de hecho la LOPD[5] no regula su tratamiento, aunque la Constitución Española[21] en su artículo 18 estipula lo siguiente:

        "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen."

    4. Si estas imágenes se guardan, a la hora de eliminarlas se deberán tratar según corresponda en función del soporte utilizado:

        En las imágenes grabadas o tomadas con móviles, PDAs, cámaras de fotos y similares se procederá a la destrucción de las tarjetas o memorias tal como se ha explicado anteriormente.

        Si se han utilizado otros medios como por ejemplo videocámaras de seguridad y los datos están almacenados en cintas se deberá proceder a su destrucción física ya que

los magnetizadores de cinta no garantizan que sea imposible la recuperación.

5. Es importante indicar que además de las leyes de carácter general[3,5,21] ya nombradas existen otras específicas que regulan la utilización de videocámaras[22-26].

5 Empresas y *Software*.

Existen varias empresas en España dedicadas a la destrucción de información confidencial. Ejemplos de ellas son las siguientes:

Deletedoc	http://www.deletedoc.com/
D+S	http://www.destruseg.es/
Reduce	http://www.reduce.es/
Safetydoc	http://www.safetydoc.es/
Eco Shredder	http://www.eco-shredder.com/
Destrupack	http://www.destrupack.com/
Tritura	http://www.tritura.net/+
Reciclajes Dolaf	http://www.reciclajesdolaf.com/

La asociación española que engloba a las empresas de destrucción de información confidencial es la AEDCI (http://www.aedci.es/).

Entre el *software* de borrado existente, podemos mencionar los siguientes programas:

Disk Wipe	http://www.diskwipe.org/
Freeraser	http://www.codyssey.com/
DISKExtinguisher	http://www.lc-tech.com/software/diskexwindetail.html
Master Shredder	http://intercrypto.com/master-shredder/
…Killdisk	http://www.killdisk.com/

6 Casos de estudio

- **Título de la sentencia:** La Guardia Civil devuelve un ordenador incautado con documentación confidencial de la propia Guardia Civil.

- **Año de la sentencia**: Abril 2008.

- **Exposición de hechos**: En 2001, con motivo de la denominada operación "Mediterráneo", se detuvo a D. X.X.X., a quien se le incautaron 2 ordenadores y una cámara fotográfica por parte de la Guardia Civil para su estudio. D. X.X.X. fue condenado a un año de prisión como cómplice de un

delito contra la salud pública. Saldada su deuda con la justicia, consiguió que en 2005 se ordenase la devolución del material que le fue incautado**.**
Con los ordenadores y la cámara en su poder, intentó recuperar sus antiguos documentos utilizando alguna aplicación de recuperación de ficheros, y lo cierto es que la aplicación debió funcionar bien porque recuperó cientos de documentos confidenciales de investigaciones de la Guardia Civil en relación a seguimientos de sospechosos y escuchas telefónicas entre otras cosas. Además, en la tarjeta de memoria de la cámara encontró decenas de fotografías de investigados y sospechosos.
Resulta evidente que el material informático fue utilizado por la Guardia Civil durante el tiempo que permaneció incautado**,** y que una vez devuelto no tuvieron las diligencias oportunas para evitar el recuperado de información, y que por otra parte no cumplía con las medidas de seguridad exigidas por ley porque, según manifestaciones de la Guardia Civil, esos ordenadores no fueron conectados a la red corporativa y por tanto no era necesario instalar medidas de seguridad.

- **Qué leyes se han aplicado**: La Dirección General de la Policía y de la Guardia Civil ha infringido lo dispuesto en el artículo 10 de la LOPD, infracción tipificada como muy grave en el artículo 44.4.g) de de la citada Ley Orgánica.

- **Resultado**: la consecuencia jurídica de que una Administración Pública vulnere la Ley Orgánica de Protección de Datos es simplemente esa: declarar que se ha cometido una infracción, pero no hay, en absoluto, multas pecuniarias ni ninguna otra sanción. Si esta misma infracción se le hubiera imputado a una entidad privada o a un particular responsable del fichero, seguramente la sanción habría sido una multa de 300.000 euros, pero en el caso de tratarse de Administraciones Públicas, simplemente se hace un escrito que pone "*Declarar que la Dirección General de la Policía y de la Guardia Civil ha infringido lo dispuesto en el artículo 10 de la LOPD, tipificada como muy grave en el artículo 44.4.g) de de la citada Ley Orgánica*".

- **Comentario crítico:** Aunque las consecuencias de infringir la LOPD no son las mismas para las Administraciones Públicas que para el resto, no les exime de cumplirla y de dar ejemplo, ya que con casos como el que se ha descrito su credibilidad puede quedar en entredicho.

7 Conclusiones

Este estudio de los peligros y consecuencias asociadas a no eliminar los datos confidenciales lleva a recapacitar sobre la necesidad de disponer de una normativa centralizada relativa a la destrucción que dependa del nivel de confidencialidad de la información global.

Esta normativa debe asegurar que los dispositivos electrónicos serán tratados adecuadamente utilizando un borrado seguro, en lugar de un simple formateo, posteriormente se deberá confirmar la desaparición real de la información. De la misma manera en caso de no poder hacer un borrado, por ejemplo cuando el soporte utilizado es el papel, teléfonos móviles, etc; en tal caso se procederá a la destrucción física del elemento en cuestión, y esta deberá ser llevada a cabo "in-situ" para evitar problemas durante el transporte con la cadena de custodia.

Si para llevar a cabo las tareas anteriormente descritas se contrata a una empresa externa se deberá explicitar en el contrato cómo deben destruir, qué medidas de seguridad son necesarias, etc, y exigir siempre un certificado donde conste qué se ha destruido y el método utilizado.

Para facilitar la tarea de auditar el proceso de eliminación será muy útil la existencia de registros donde figure la petición de destrucción, la retirada del material, la recepción de este y la notificación de que el proceso ha concluido satisfactoriamente.

En una línea más orientada hacia la docencia el caso más práctico sería el de destrucción de los exámenes, hay centros que obligan a guardarlos durante un año, aunque otros con una normativa más restrictiva lo hacen durante cinco, pero este asunto queda fuera del ámbito de este trabajo. Lo importante es atenerse a lo estipulado de manera que en caso de reclamación o litigio se hayan cumplido dichos plazos.

Véase por ejemplo la sentencia dictada en 2004 a favor de la Universidad de Valencia a la cual se le había interpuesto una reclamación de Responsabilidad Patrimonial mediante un recurso contencioso-administrativo por la destrucción del examen de un alumno después de haber transcurrido un año y casi cuatro meses de su realización. El interesado pretendía que se comparase su examen con el de sus compañeros para demostrar el excesivo rigor aplicado en la corrección.

Puesto que dichos documentos ya no existían y no se tenía la certeza de que en caso de ser así se hubiera podido probar tal hecho, se exime de toda responsabilidad a la Universidad y no se impone a la indemnización de 3.067,30 euros solicitada.

Bibliografía

[1]. Decisión Nº 1600/2002/CE del parlamento europeo y del consejo de 22 de julio de 2002, por la que se establece el Sexto Programa de Acción Comunitario en Materia de Medio Ambiente.
http://www.maec.es/SiteCollectionDocuments/Espana%20y%20la%20Union%20Europea/Politicas%20Comunitarias/MedioAmbiente/VIProgramaMedioAmbientePDF198Kb.pdf

[2]. Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
https://www.sede.fnmt.gob.es/sede/normas/Directiva-95-46-CE.pdf

[3]. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
http://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

[4]. Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad en los ficheros automatizados previstos en el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio
http://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/A.9-cp--Real-Decreto-195-2000.pdf

[5]. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf

[6]. Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
http://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/A.8-cp--Real-Decreto-994-1999.pdf

[7]. Ley 10/1998, de 21 de abril, de residuos.
http://www.arc.cat/ca/publicacions/pdf/normativa/espanyola/leyes/ley_10_1998.pdf

[8]. Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/autonomica/common/pdfs/A.19-cp--Ley-8-2001.pdf

[9]. Guía de seguridad de datos publicada en 2008 por la AEPD
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

[10]. Organización Mundial de la Propiedad Intelectual
http://www.wipo.int/sme/es/documents/disclosing_inf.htm#P15_532

[11]. Multa de 60.000 € a BBVA por el abandono de datos confidenciales en un descampado
http://www.elmundo.es/elmundo/2008/04/19/castillayleon/120857770.html

[12]. La Unidad de Investigación del Clima (UIC) de la Universidad británica de Anglia del Este denunció el robo de información y correos electrónicos que posteriormente fueron publicados.
http://ntrzacatecas.com/noticias/mundo/2009/11/22/denuncia-universidad-robo-de-informacion-sobre-cambio-climatico/

[13]. Audiencia Nacional. Sentencia de 23-03-2006. Sala de lo Contencioso-Administrativo, sección primera. Incumplimiento de las medidas de seguridad en la destrucción de documentos.
https://www.agpd.es/portalweb/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia-AN-23-03-2006.pdf

[14]. Audiencia Nacional. Sentencia de 23/03/2006. Incumplimiento de las medidas de seguridad. Documentos encontrados en el contenedor de una obra
http://www.google.es/url?sa=t&source=web&ct=res&cd=3&ved=0CBkQFjAC&url=http%3A%2F%2Fwww.tirea.es%2FHome%2FSeguridadyProteccionde Datos%2FSentencias%2Ftabid%2F299%2FDMXModule%2F860%2FCommand%2FCore_Download%2FDefault.aspx%3FEntryId%3D3092&rct=j&q=Audiencia+Nacional+APD+destrucci%C3%B3n+de+datos&ei=WUZjS_6tCIvR4gbP8enTBg&usg=AFQjCNFdVBSukM61Oozm3oipNSK35cAr7g

[15]. El robo de información confidencial en las empresas aumentó en un 60% en 2008, según el Grupo Paradell
http://ugtsecsindicalsecuritasvic.blogspot.com/2009/07/el-robo-de-informacion-confidencial-en.html

[16]. Método Gutmann
http://en.wikipedia.org/wiki/Gutmann_method

[17]. Recomendaciones para la destrucción física de documentos de archivo en papel de la Administración General del Estado
http://www.reciclajesdolaf.com/Recomendaciones%20para%20la%20destrucci%C3%B3n%20f%C3%ADsica%20de%20documentos%20de%20archivo.pdf

[18]. Dumpster diving
http://www.fcanals.com/contenidos/terminos/dumpsterdiving.htm

[19]. Dumpster diving
http://en.wikipedia.org/wiki/Dumpster_diving

[20]. Liberalia tempus. Servicios informáticos
http://www.liberaliatempus.com/secure-delete.html

[21]. Constitución Española 1978
http://noticias.juridicas.com/base_datos/Admin/constitucion.html#

[22]. Real Decreto596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos
http://noticias.juridicas.com/base_datos/Admin/rd596-1999.html

[23]. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
http://noticias.juridicas.com/base_datos/Admin/lo4-1997.html

[24]. Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.
http://noticias.juridicas.com/base_datos/Admin/lo1-1992.html

[25]. Ley 23/1992, de 30 de julio, de Seguridad Privada
http://noticias.juridicas.com/base_datos/Admin/l23-1992.html

[26]. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.
http://noticias.juridicas.com/base_datos/Admin/rd2364-1994.html#