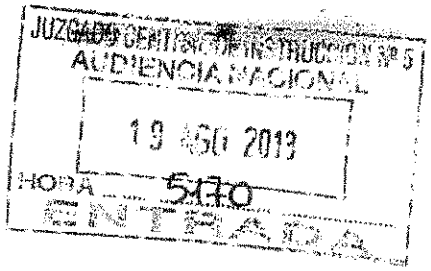
JUZGADO CENTRAL DE INSTRUCCIÓN Nº 5
AUDIENCIA NACIONAL
DILIGENCIAS PREVIAS 275/2008
PIEZA SEPARADA "INFORME UDEF-BLA Nº 22.510/13".



Madrid, 20 de agosto de 2013.

En cumplimiento del requerimiento del Ilmo. Sr. Magistrado Juez del Juzgado Central de Instrucción Número 5 de la Audiencia Nacional, de fecha 16 de agosto de 2013, por el que se solicita la puesta a disposición de ese Juzgado de *"los dos ordenadores portátiles que Luis Bárcenas Gutiérrez hubiera ostentado en dicha sede"*, cúmpleme informar lo siguiente:

Primero.- Sobre la titularidad de los ordenadores.

El Juzgado de Instrucción número 21 de Madrid, mediante Auto de fecha 21 de abril de 2013, recaído en Diligencias Previas 604/2013-D, acordó el sobreseimiento libre y archivo de la denuncia formulada por Luis Bárcenas contra el firmante de este escrito por supuesto robo de los dos ordenadores en cuestión.

Según consta en el indicado procedimiento, el denunciante manifestó no poder acreditar su propiedad sobre los ordenadores, cuya marca y modelos ni siquiera pudo reseñar.

De acuerdo a los antecedentes que he podido recabar, resulta que Luis Bárcenas tuvo asignado el uso de varios ordenadores pero no ha "ostentado" como propio ningún equipo informático del Partido, desconociendo el firmante si además utilizaba algún otro equipo de su propiedad que se encuentre en la actualidad a su disposición.

En particular, resulta que Bárcenas tuvo asignados a su uso dos ordenadores portátiles marca TOSHIBA y APPLE, respectivamente.

2.- Sobre el estado actual de los ordenadores portátiles.

De conformidad con el protocolo habitual de utilización y reciclaje de material informático, cada vez que se deja de utilizar un equipo asignado a una persona, se reintegra al sistema general, para reformatearlo y disponerlo para su posible asignación a otro usuario. Esta práctica se aplica también a medios de almacenamiento masivo de información, cualquiera que sea su formato, tales como *pen drives, CD, DVD,* discos duros externos, etc. En caso de equipos que hayan sido utilizados por personas que hubieran podido manejar información sensible, se procede a la destrucción de los sistemas de almacenamiento, de acuerdo al protocolo que se aporta.

Se acompaña, en efecto, a este escrito explicación del procedimiento que se sigue en el Partido Popular, de acuerdo con la "Guía sobre almacenamiento y borrado seguro de información", elaborada por el equipo del Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnología de la Comunicación, INTECO, del Ministerio de Industria, Turismo y Comercio, la Ley Orgánica 15/1989, e 13 de diciembre, y el Real Decreto 1720/2007, de 21 de diciembre.

En todo caso, interesa hacer dos puntualizaciones adicionales:

a) Por lo que se refiere al ordenador marca APPLE, según consta en el procedimiento seguido ante el Juzgado de Instrucción número 21 de Madrid, el disco duro de este ordenador fue sustituido por Luis Bárcenas en el mes de octubre de 2012, manifestación que reiteró el imputado ante ese Jugado de Instrucción número 5 de la Audiencia Nacional, según se ha filtrado a la prensa, por lo que el Partido no ha tenido a su disposición el citado disco, sino el nuevo que el imputado instaló en octubre de 2012, y que ha sido destruido de acuerdo a lo indicado anteriormente, para su puesta en uso por otra persona.

b) En cuanto al ordenador marca TOSHIBA, constan manifestaciones del imputado también filtradas a la prensa, según las cuales determinada información que fue entregada ante ese Juzgado habría sido extraída a un *pen drive* desde del citado ordenador; esta afirmación es absolutamente falsa porque este ordenador, por su antigüedad, carece de puerto USB alguno.

En consecuencia, de conformidad con los indicados protocolos, los discos duros de los ordenadores de Luis Bárcenas fueron destruidos, una vez alcanzada

firmeza la resolución judicial que denegaba su devolución al denunciante por no haber acreditado la propiedad de los mismos.

En las condiciones que se han explicado en este escrito, se ponen a disposición del Juzgado los dos ordenadores solicitados.

Es cuanto tengo el honor de informar a ese Juzgado, quedando a su disposición para cualquier aclaración complementaria que proceda.

Alberto Durán Ruiz de Huidobro
Abogado

PROCEDIMIENTO DE BORRADO SEGURO (BS)

Este procedimiento será de aplicación a cualquier tipo de dispositivo que almacene información y que haya sido utilizado por un usuario de la Entidad.

Pasos

1) *Determinación del nivel de criticidad*: Se establecerá en función de la condición del usuario y del valor estratégico de la información que éste pueda manejar. Si el nivel de criticidad resultante es bajo, el dispositivo una vez borrado de forma segura (BS), será reutilizado. En el caso de que el nivel de criticidad resultante sea medio o alto, una vez ejecutado el procedimiento de BS, se procederá a su destrucción física en la medida y forma necesarias, para en cualquier caso se puedan evitar métodos de lectura avanzados sobre dispositivos dañados.

2) *Nivel de aislamiento del dispositivo:* Éste deberá ser desmontado –en la medida de lo posible- de cualquier sistema al que pudiera estar ligado (PC de sobremesa, Portátil, Array, Teléfono, etc.) de forma que pueda ser conectado y accedido en forma de esclavo a un sistema controlado por la entidad y que actuará como maestro. La idea es acceder al dispositivo esclavo sin que sean necesarias credenciales sobre el mismo. Como punto a destacar y en función del nivel de confianza sobre el dispositivo a borrar, se deberá aislar el sistema maestro de la propia red y sistemas de la entidad.

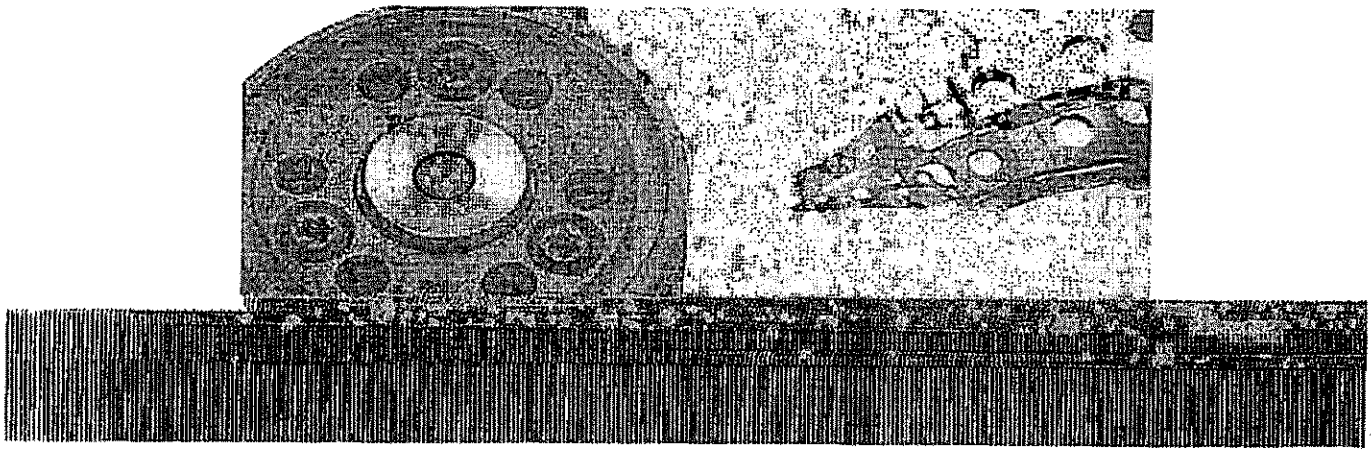
3) *Borrado seguro:* El BS se realizará con herramientas de escritura a bajo nivel y en reiteradas pasadas. El objetivo será tender a 35 pasadas –según método Gutmann-.

4) *Destrucción o reciclado:* En función del nivel de criticidad resultante del punto primero, el dispositivo será destruido o reciclado.

    a. En el primer caso, se dañará el dispositivo de forma que éste pierda su integridad. Por poner unos ejemplos, Las llaves USBs, DVDs y CDs serán destruidos por aplastamiento; los discos magnéticos de los HDs, desmontados, rayados y destruidos; los teléfonos, destruidos o donados al propietario; etc. Como punto a destacar, los elementos resultantes serán depositados en varios contenedores habilitados al efecto.

    b. En el segundo caso, se devolverá el dispositivo al Dpto. Sistemas de Información para su reutilización.

Guía sobre almacenamiento y borrado seguro de información



Edición: Abril 2011

La "Guía sobre almacenamiento y borrado seguro de información" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Susana de la Fuente Rodríguez

5.3 LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD)

La **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD)**, obliga a las empresas a custodiar la información de modo que no pueda ser accedida por terceros no autorizados. Hace referencia a la legislación aplicable en cuanto al uso y difusión de datos personales de un tercero sin previa autorización (por ejemplo, publicar fotografías de un cliente en el perfil social de la empresa o difundir datos personales de un socio empresarial sin previa autorización, entre otros).

Además, es importante tomar en consideración que las empresas e instituciones de cualquier tamaño son responsables de todos los datos informáticos almacenados en sus equipos. Cada día más, los empleados almacenan grandes cantidades de información en los discos duros de sus equipos informáticos, que en muchos casos, contienen a su vez datos personales o privados que les confieren características de confidencialidad. La eliminación no segura de la información puede ocasionar una posterior recuperación no autorizada, ocasionando grandes perjuicios comerciales, de imagen y, por supuesto, legales.

El **Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal (RDLOPD)** desarrolla de forma completa la LOPD.

Específicamente en el artículo 92.4 se expone lo siguiente: *siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.*

Las sanciones[11] por el incumplimiento de obligaciones legales en materia de protección de datos pueden variar entre 900 euros a 40.000 euros (infracciones leves), entre 40.001 a 300.000 euros (infracción grave) y entre 300.001 a 600.000 euros (infracción muy grave), siendo la Agencia Española de Protección de Datos la entidad encargada de su aplicación.

Por las razones expuestas anteriormente, es de gran importancia realizar un borrado seguro de datos, no sólo desde el punto de vista de la privacidad de los usuarios y la seguridad de las empresas, sino que, además, constituye una medida de obligatorio cumplimiento cuando se trata de datos de carácter personal, según lo estipulado en la LOPD y el RDLOPD.

[11] Modificación de la Ley de Protección de Datos de Carácter Personal (LOPD), contenida en la Ley 2/2011, de 4 de marzo, de Economía Sostenible. Disponible en: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-4117