Sanitización y Eliminación de Medios de Almacenamiento

Sarah Bracho ~ Nicolás Patalagua

sarahbracho1703@gmail.com ~ nicopatalagua@gmail.com

Resúmen: *El mundo actual, implica un flujo y recolección de información por diversas actividades de la vida cotidiana, dicha información en un 98% es almacenada. La información almacenada supone ser necesaria y vital para diversas organizaciones o personas, pero se rige por un ciclo de vida que termina con su destrucción. La destrucción de la información desde la seguridad informática es una actividad de alta importancia, que requiere de métodos de destrucción de información que no solo borren los contenidos de la lista de archivos sino que logren la eliminación de contenidos específicos en la zona de almacenamiento.*

Abstract: *The current world, involves a flow and collection of information by various activities of daily life, such information in 98% is stored. The stored information supposes to be necessary and vital for diverse organizations or people, but it is governed by a life cycle that ends with its destruction. The destruction of information from computer security is a highly important activity, which requires information destruction methods that not only erase the contents of the file list but also record the destruction of specific contents in the storage area.*

Palabras clave: *Información, destrucción certificada, desmagnetización. destrucción física, sobre-escritura, borrado seguro, purga de información, sanitización, eliminación medios de almacenamiento, medios de almacenamiento.*

Keywords: *Information, certified destruction, demagnetization. physical destruction, overwriting, secure deletion, information purging, sanitization, deletion of storage media, storage media.*

I. INTRODUCCIÓN

Un activo para la mayoría de organizaciones está basada en la información recolectada por diversas actividades, para su posterior tratamiento, manipulación, análisis y sobre todo *almacenamiento.* La información es un conjunto de datos que han sido procesados y ordenados, esta información puede encontrarse de dos formas: información digital contenida en flash USB, discos magnéticos, CD's, tarjetas de memoria entre otros, y la información tradicional contenida en documentos, papeles, carpetas, entre otros.

Tanto la información digital como la información tradicional cumplen con un ciclo de vida, que consta de tres fases: la generación de esta información, la transformación y tratamiento y finalmente llega a su fin con la destrucción de la misma, este último implica el uso de medios, mecanismos y métodos de borrado y destrucción con el fin de que la información no llegue a ser reciclada y reutilizada con fines distintos por parte de terceros.

Imagen 1: Ciclo de vida de la información

De forma contextual, la destrucción de datos trae consigo la necesidad de realizar una eliminación de forma segura o realizar la sanitización de los dispositivos, con el fin de restringir el acceso a los datos, debido a que la información al no ser eliminada de forma segura tiende a ser reutilizada, revendida o reparada. Lo cual puede conllevar sanciones legales, costos por la conservación y la custodia de la información, daños en la imagen causada por la divulgación de la misma o simplemente riesgos de robo o uso indebido de información que se considere de carácter privativo o confidencial.

II. MARCO TEÓRICO

Información

Idalberto Chiavenato considera que la información es un conjunto de datos con un significado, que reduce la incertidumbre y aumenta el conocimiento de algo.[1]

Por su parte, en el libro *La revolución de la riqueza,* los autores Alvin y Heidi Toffler advierten sobre una notoria y muy extendida diferencia entre la información y los datos, los cuales suelen ser confundidos. Ellos consideran que los datos generalmente estas descritos como elementos discretos o sin un contexto particular, sin embargo cuando estos son contextualizados se convierten automáticamente en información.[2]

Podemos tener estos y otras definiciones de lo que es la información, como podría demostrarse con la definición que se ofrece en el diccionario de la Real Academia Española, en el cual la información tiene 8 definiciones aceptadas y para

acciones y contexto de este documento usaremos la número 5: *"Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada."*[3]

Pero ¿Porqué es tan importante la información?, pues bien la información siempre ha sido un recurso importante tanto para organizaciones como también para personas, que durante mucho tiempo han tratado y han requerido almacenarla como una necesidad tanto para el conocimiento como para la preservación de su cultura o tradiciones. Y bien, en la actualidad es un objeto que forma parte del marketing y el mercado digital, es decir la información se compra y se venda, brindando beneficios reales tanto financieros como políticos, sociales y culturales. Es por ello que se deben contar con una serie de normas y protocolos de lo que conocemos como seguridad de la información, que como bien lo indica hace referencia a la medidas que se toman tanto en sistemas de información como en bancos de datos, bases de datos, dispositivos de almacenamiento, entre otros para preservar la confidencialidad, la integridad, la disponibilidad y sobre todo la autenticación de la misma.[4]

Medios de almacenamiento

Como ya sabemos la información puede encontrarse de dos formas: *tradicional* y *digital.* El almacenamiento tradicional implica un almacenamiento físico en bancos de documentos, centros de archivo y demás, mientras que la información digital requiere de dispositivo o medios de almacenamiento tanto físicos como lógicos, es decir puede almacenarse en aparatos de uso cotidiano diseñados para tal motivo o bien pueden ser almacenados en servidores de nubes a las cuales no tenemos acceso pero sí fisico a traves de credenciales de usuario o contraseñas preestablecidas.[5]

En primer lugar es necesario aclarar que un medio de almacenamiento, es un dispositivo periférico de un sistema de información que actúa como soporte de grabación de la información y de datos en general. Es decir los datos o información usada por parte de ordenadores, sistemas y/o aplicaciones requiere de un sitio donde almacenarse durante su ciclo de vida. Generalmente la información se almacena en la RAM(Random Access Memory) o memoria de acceso aleatorio, pero dicha memoria requiere de alimentación constante para preservar la información por lo cual es necesario llevar esta información a espacios donde la información quede alojada una vez el dispositivo de procesamiento sea apagado. [6]

Los dispositivos usados para este fin pueden incluir desde tarjetas y cintas perforadas (no usadas actualmente), soporte magnético de almacenamiento, soporte óptico de almacenamiento, soporte magneto-óptico de almacenamiento o bien soporte de estado sólido.[7]

Entre los dispositivos magnéticos caracterizados por usar propiedades magnéticas en especial en los tambores formados por cilindros, encontramos cintas magnéticas, DAT (Digital Audio Tape), DDS (Digital Sata Storage), DLT (Digital Linear Tape), LTO (Linear Tape-Open), discos magnéticos, FDD (floppy disc) o disquetes (Obsoletos hoy en día), y los conocidos discos duros.[7]

Para el almacenamiento óptico, que usan discos que almacenan la información en surcos microscópicos con un láser, existen dispositivos como LD o discos láser, CD's o discos compactos, DVD (Disco versátil digital) y los ya casi extintos BD o discos blu-ray. El almacenamiento en disco magneto-óptico se basa en discos ópticos que son capaces de escribir y reescribir datos sobre sí mismo, como es el caso de los discos Zip, Jaz, Minidisc y los muy distribuidos SuperDisk. [7]

Por último están las unidades de estado sólido o SSD, que basan su funcionamiento en el uso de memoria no volátil, algunos ejemplos de este tipo de almacenamiento son las memorias flash, las memorias con puerto USB, las tarjetas de memoria, las SD o secure digital, las MS o memory stick, las MMC o multimediacard, las MD o microdrive y las SM o Smartmedia, que se usan junto a las XD picture.[7]

Destrucción certificada

Según la norma UNE 15713 del *Organismo Internacional de Estandarización (ISO),* se estipulan una serie de protocolos y recomendaciones para realizar la gestión y control de temas relacionados con la destrucción segura de material confidencial de forma segura y libre de sanciones, este código de buenas prácticas proporciona recomendaciones a ser aplicadas por las dependencias encargadas de la custodia de material confidencial en las organizaciones, de igual forma regula los procesos de destrucción de información que contiene datos personales.[8]

Esta norma cuenta con 4 fases de acción: desde el momento que es recolectada la información, la llegada a las instalaciones, la destrucción de la información y sus documentos y finalmente la emisión de un certificado de *"Destrucción certificada"*. [8]

Nota: La destrucción certificada, es decir con garantías de seguridad y confidencialidad, está normalizada según las normas UNE-EN 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas y DIN 66399. Se tipifican soportes, métodos de destrucción y niveles de protección y de seguridad. [9]

Limpieza o borrado seguro

El ciclo de vida de la información, como se evidencia en la introducción del documento tiene su ocaso en la destrucción de la misma, este es uno de los factores más importantes de la seguridad de la información en una empresa y sus motivos o causas pueden ser diversos, aunque algunas empresas reguladas por leyes vigentes en el país deben conservar cierta información por un periodo de tiempo determinado antes de tomar la decisión de eliminarla por completo. Es por esto que surgen una serie de métodos, prácticas y formas de garantizar que al momento de tomarse la decisión final de eliminarse se realice de tal forma que no se pueda reciclar o recuperar.[9]

Algunos métodos como el *tecla supr* o *delete,* no realizan un borrado seguro, esto porque solo eliminan los archivos de *la lista de archivos*, más no eliminan el contenido del archivo a razón que este se almacena en la *zona de almacenamiento,* hasta el momento que este lugar se reemplace o reutilice con un nuevo documento.[8]

Desmagnetización

Quizá uno de los métodos de borrado seguro más usados, porque evita la recuperación de los datos contenidos en los dispositivos o medios de almacenamiento. La desmagnetización ocurre cuando el dispositivo donde se encuentra almacenada la información sufre los efectos de un campo magnético de alta potencia.[8]

Este método es eficiente para dispositivos de soporte de almacenamiento magnético ya antes referenciados; sin embargo se debe tener en cuenta que cada dispositivo requiere una potencia de campo magnética específica para que se asegure una polarización efectiva en cada una de las partículas y espacios de memoria.[8]

Destrucción física

Una práctica bastante costosa pero eficiente es la destrucción física porque deja inutilizado el soporte de almacenamiento de cualquier tipo, esta práctica puede ejecutarse con la desintegración del dispositivo, la pulverización, la fusión e incineración, las cuales se realizan clandestinamente o en una planta destructora de metal que tenga autorización.[8]

Sobre-escritura

Según el grupo Urbegi con sede en Balmaseda, la sobreescritura para seguridad de la información consiste en la escritura de un patrón de datos contenidos en los medios de almacenamiento, con el fin de asegurar la completa destrucción de los datos se debe realizar una sobreescritura en la totalidad de la superficie del dispositivo de almacenamiento. [9]

Este procedimiento se logra accediendo al contenido y en primer lugar a la información almacenada en los dispositivos de soporte de almacenamiento, modificando los valores almacenados, sin embargo no puede ser usado en dispositivos dañados o que no brinden la posibilidad de ser regrabables.[9]

Destrucción Física	Desmagnetización	Sobre-escritura
Forma segura	Forma Segura	Forma Segura
Destrucción para cada soporte	Destrucción para cada soporte	Una solución para todos los soportes
Dificultad en certificación	Dificultad en certificación	Garantía documental de la operación
Necesidad de transporte a ubicación externa	Necesidad de transporte a ubicación externa	Eliminación en el sitio de almacenamiento
No se garantiza cadena de custodia	No se garantiza cadena de custodia	Se garantiza cadena de custodia
Destrucción definitiva	Destrucción definitiva	Reutilización

Tabla 1: Comparación métodos borrado seguro[10]

Soporte	Destrucción física	Desmagnetización	Sobre escritura
Disco duro	◉	◉	◉
Discos flexibles	◉	◉	◉
Cintas de backup	◉	◉	◉
CD	◉		
DVD	◉		
Blu-ray Disc	◉		
Pen Drive	◉		◉
Discos SSD	◉		◉

Tabla 2: Método de borrado adecuado en función del dispositivo[10]

Nota: A pesar que actualmente la sobre-escritura es un método seguro de destrucción de datos para dispositivos basados en memorias de estado sólido, diversos trabajos de investigación forense apuntan la posibilidad de recuperación posterior con técnicas de lectura directa de los chips de memoria. Uno de estos estudios es el de la Universidad de California http://nvsl.ucsd.edu/sanitize/.presas.com/gestion-de-documentos/la-normativa-vigente-para-la-destruccion-de-documentos [10]

III. OBJETIVO

El objetivo principal de la sanitización y esterilización de medios es que las organizaciones, empresas y personas en general cuenten, conozcan y apliquen políticas de borrado

seguro de la información que almacenan en los dispositivos de soporte de almacenamiento con los que cuentan y trabajan. Para esto es necesario realizar estrictos controles de seguimiento de estos dispositivos, además de una eficiente supervisión de los mismos, para que cualquier operación realizada en estos dispositivos cuente con una trazabilidad del funcionamiento de los mismos. Es importante tener en cuenta los estándares para **cadena de custodia** cuando los dispositivos de almacenamiento se encuentran relacionados en procesos legales o simplemente porque son trasladados a instalaciones externas a la organización.

Por su parte se debe llevar también un control de la documentación y la certificación de operaciones de borrado seguro que se realicen. Es decir al momento de optar por una herramienta de borrado seguro es necesario que dicha opción brinde un soporte o documento que identifique claramente el proceso de borrado.

Nota: Toda empresa debe contar con una política de borrado seguro de la información de los dispositivos de almacenamiento con los que trabaja.[10]

IV. HERRAMIENTAS

El INCIBE (Instituto Nacional de ciberseguridad de España, fundada en 2006, dedicada al soporte en materia de seguridad informática de los ciudadanos, empresas públicas y privadas,y administraciones públicas y organismos relacionados, asimismo a las instituciones académicas e investigativas, tiene un catalogo se soluciones de seguridad, productos y servicios en el mercado español, acerca del almacenamiento y borrado seguro siguiendo lineamientos de cumplimiento legal como lo es la *Ley Orgánica de Protección de Datos, Ley de Servicios de la Sociedad de la Información* y la *Ley de Propiedad intelectual*, entre muchas otras. También se hace énfasis en técnicas de borrado seguro y destrucción documental, y prevención de fuga de información gestionando el ciclo de vida de la información.[11]

Como se evidencia en varios puntos de este documento, eliminar información es una tarea importante, en especial cuan do la información es confidencial o muy privada. [12]

Por este motivo se seleccionó una serie de herramientas que se usan para eliminar datos de cualquier dispositivo de soporte de almacenamiento, haciendo los archivos irrecuperables:[13]

1. Hardwipe
2. KillDisk
3. PcDiskEraser
4. HDDErase
5. HDShredder Free Edition
6. Darik's Boot
7. Nuke
8. Clean Disk Security
9. Easis Data Eraser
10. CBL Data Shredder
11. CCleaner
12. Eraser
13. Intel Solid State Toolbox
14. Corsair SSD Toolbox
15. SanDisk SSD Toolbox
16. Samsung Magician Software
17. OCZ Toolbox

V. PROCEDIMIENTO

Sanitización de medio externo

1. Usando el software "Hardwipe" instalado en un sistema operativo Windows (Imagen 2).

Imagen 2: Hardwipe instalado en Windows

2. Posteriormente se selecciona el botón *"Dispositivos"*, para seleccionar el dispositivo sobre el cual vamos a realizar la sanitización. (Imagen 3)

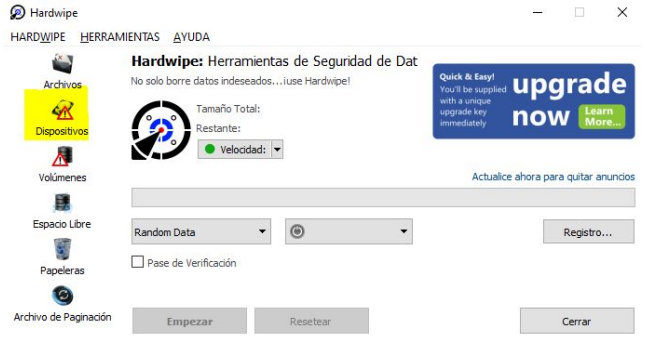

Imagen 3:Botón dispositivos

3. Se selecciona el dispositivo al cual se realizará santificación marcando la casilla, en este caso la "Disco 1" (Imagen 4). Y se da clic en *Aceptar*.

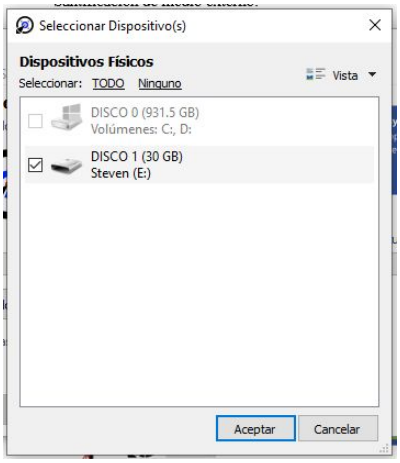

Imagen 4:Selección del disco externo

4. Ahora se selecciona el algoritmo de borrado seguro a utilizar, para este caso se usa DoD 5220.22-m. (Imagen 5)

Imagen 5: Selección de algoritmo

5. Se da clic en empezar y esto inicia el proceso de borrado seguro como se ve en la *Imagen 6.*

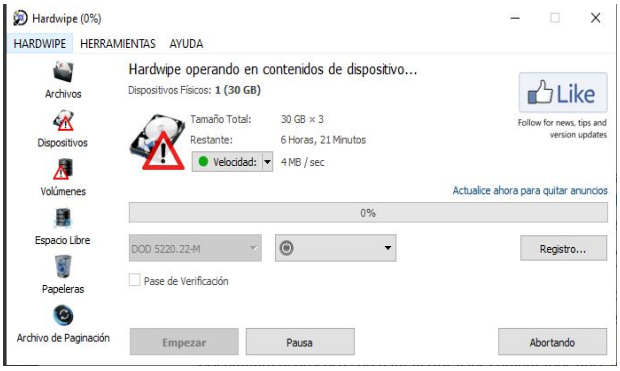

Imagen 6: Proceso de borrado seguro

6. Obtener una imagen forense del dispositivo con el programa FTK Imager Lite. (Imagen 7)

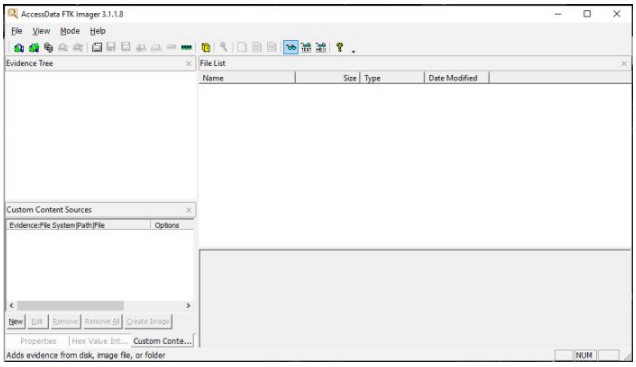

Imagen 7: FTK Imager Lite

7. Para crear la imagen del dispositivo se da clic en el botón resaltado en la imagen 8.

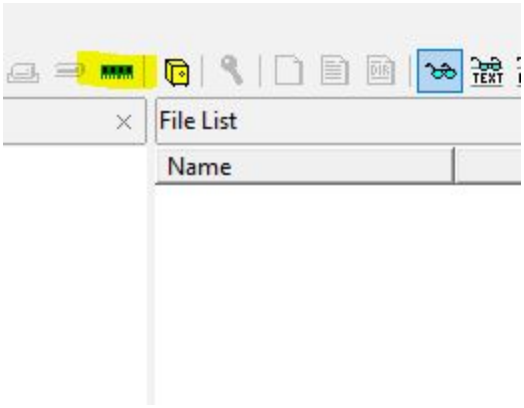

Imagen 8: Botón crear imagen forense

8. Luego se solicitara la unidad en donde se va a generar la imagen de memoria, en este caso será en E:\ como se detalla en la imagen 9.

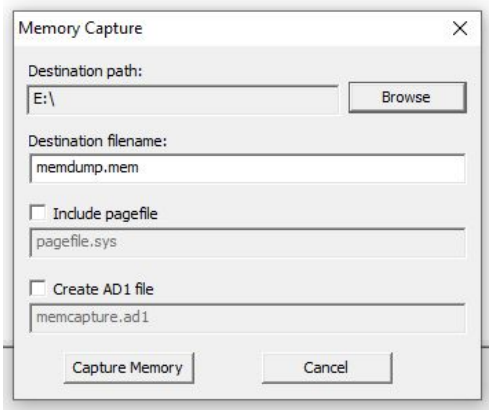

Imagen 9: Configuración para la imagen de memoria

9. Una vez cliqueado el botón Capture Memory se muestra el progreso de captura de memoria, como se muestra en la figura 10.

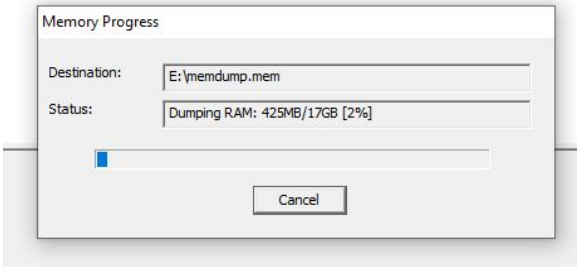

Imagen 10:Progreso de captura de memoria

VI. RESULTADOS

Luego de haber realizado los pasos indexados anteriormente, se genera un archivo de formato *.mem,*el cual es la imagen de memoria generado por el programa FTK imager lite, como se muestra en la imagen 11. Esta es una imagen forense, la cual es una copia bit a bit del dispositivo de almacenamiento de 32 Gb, que hemos seleccionado, el cual fue sometido a un proceso de esterilización que llevo casi 6 horas.

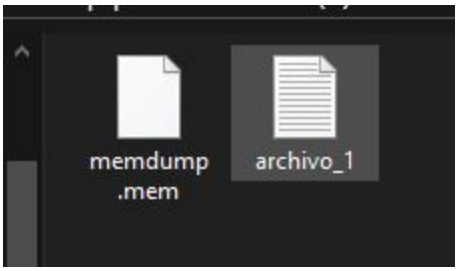

Imagen 10:Imagen de memoria

En la imagen forense, se copiaron todos los espacios del medio de almacenamiento, sin modificar los metadatos, ni siquiera hubo modificaciones en las fechas, ni en las horas. Es por esta razón que son una herramienta importante para los procesos judiciales a razón de que preservan la información de forma inalterada, garantizando veracidad de los documentos o pruebas presentadas.[14]

Al realizar la creación de la imagen forense se evidencia que lleva un consumo de tiempo bastante alto, por lo cual es recomendable realizarse con antelación cuando es requerida para presentarse como prueba ante un tribunal. Se debe tener en cuenta que para realizar dicha imagen se debe tener una autorización legal o en su defecto una orden de registro.[15]

VII. CONCLUSIONES

Al finalizar esta investigación se puede llegar a la conclusión que la información puede sufrir consecuencias de reutilización, venta de la misma, reparacion de información delicada con fines ilícitos, la eliminación sin consentimiento, la destrucción de la información y los aparatos que la contienen. También se debe hacer énfasis en la necesidad de las empresas para crear planes, procesos y tener presupuestos destinados a la sanitización de la información con el fin de administrar riesgos futuros relacionados con la falta de protección de la información, para lo cual es necesario realizar procesos de sanitización y borrado seguro con las garantías legales y técnicas correspondientes.

VIII. REFERENCIAS

[1]I. Chiavenato, *Introducción a la teoría general de la administración*. México, D.F.: McGraw-Hill, 2006.

[2]A. Toffler, H. Toffler, y J. de Jodar, *La revolución de la riqueza*. México: Debate, 2006.

[3]R.- ASALE y RAE, "información | Diccionario de la lengua española", *«Diccionario de la lengua española» - Edición del Tricentenario*. https://dle.rae.es/información (consultado abr. 09, 2020).

[4]"Criptored". http://www.criptored.upm.es/ (consultado abr. 09, 2020).

[5]"Dispositivos de almacenamiento de información", *Tecnología + Informática*, may 04, 2018. https://www.tecnologia-informatica.com/dispositivos-de-almacenamiento-informacion/ (consultado abr. 09, 2020).

[6]"Los diferentes medios de almacenamiento en informática", *Informática para tu negocio*, ago. 15, 2016. https://www.informaticaparatunegocio.com/blog/los-diferentes-medios-almacenamiento-informatica/ (consultado abr. 09, 2020).

[7]G. Beekman, *Introducción a la Informática*, 1a ed. Madrid, 2005.

[8]M. Ilundáin, "UNE 15713 Destrucción Segura del Material Confidencial". https://eqa.es/certificacion-sistemas/medio-ambiente/une-15713 (consultado abr. 09, 2020).

[9]"Reciclaje y destrucción de soportes magnéticos | Grupo Urbegi". http://urbegi.com/reciclaje-y-destruccion-de-equipos-informaticos-y-soportes-magneticos/ (consultado abr. 09, 2020).

[10]Centro Superior de Estudios de la Defensa Nacional (Espanya), *Necesidad de una conciencia nacional de ciberseguridad . La ciberdefensa: un reto prioritario.* Madrid: Ministerio de Defensa, Subdirección General de Publicaciones y Patrimonio Cultural, 2013.

[11]"INCIBE", *INCIBE*. https://www.incibe.es/ (consultado abr. 09, 2020).

[12]"INCIBE", *INCIBE*. https://www.incibe.es/ (consultado abr. 09, 2020).

[13]Y. FM, "Siete herramientas gratis para borrar de forma segura tus discos duros HDD o SSD", *Genbeta*, dic. 21, 2016. https://www.genbeta.com/herramientas/siete-herramientas-gratis-para-borrar-de-forma-segura-tus-discos-duros-hdd-o-ssd (consultado abr. 09, 2020).

[14]"Imágenes Forenses | Alonso Caballero / ReYDeS". http://www.reydes.com/d/?q=Imagenes_Forenses (consultado abr. 09, 2020).

[15]"Las imágenes forenses y su uso en procesos judiciales", *La única forma de preservar inalterada la información son las imágenes forenses.* https://www.ambitojuridico.com/noticias/tecnologia/tic/las-imagenes-forenses-y-su-uso-en-procesos-judiciales (consultado abr. 09, 2020).