Sanitización y Eliminación de Medios de Almacenamiento

Osorio, Carlos, Calderón, Alexander.
carlosjosorio, calumb10@gmail.com
Universidad Piloto de Colombia

Resumen—Se describen diferentes técnicas, métodos y consideraciones para contrarrestar la remanencia de datos en medios de almacenamiento como los discos duros, mencionando las clasificaciones más representativas de estos métodos, que hoy por hoy son utilizados, dividiéndose en cuatro categorías: eliminación, limpieza, depuración y destrucción. La eliminación es mencionada para asegurar que no todos los medios en las organizaciones requieren sanitización y que la eliminación sigue siendo un método válido para la manipulación de los medios de comunicación con información no confidencial.

Índice de Términos—Desmagnetización, Destrucción del medio, Purga de la Información, Sobrescribir, Remanencia de Datos.

I. INTRODUCCIÓN

Actualmente la clave para decidir cómo manejar los medios de almacenamiento en una organización es considerar en primer lugar la información, y luego el tipo de medio. La clasificación de seguridad de la información, junto con los factores ambientales internos, debería impulsar las decisiones sobre cómo tratar con los medios. Una vez más, la clave es pensar primero en términos de confidencialidad de la información, y luego por tipo de medio.

Muchos sistemas operativos, administradores de archivos y otro tipo de software al momento de que un usuario solicita la eliminación de un archivo, no lo realizan inmediatamente. En su lugar, el archivo es movido a un área de retención. De la misma manera muchos productos de software crean automáticamente copias de seguridad de los archivos que se están editando, para permitir al usuario restaurar la versión original, o para poder recuperarse de un posible accidente, también llamada copia de seguridad de características.

Del mismo modo, formatear, particionar o reinstalar una imagen de disco, no siempre garantiza que se escriba en todas las áreas del disco, se generaran áreas vacías cuyo contenido podrán ser archivos eliminados.

Por último, aun cuando el medio de almacenamiento se sobrescriba, las propiedades físicas de este pueden hacer posible recuperar el contenido anterior. Sin embargo, en la mayoría de los casos esta recuperación no es posible con sólo leer desde el dispositivo de almacenamiento de la forma habitual, pues requiere el uso de técnicas de laboratorio, tales como desmontar el dispositivo y acceder/leer directamente a partir de sus componentes

II. REMANENCIA DE DATOS

Es la representación residual de los datos que se mantiene incluso después de que se han hecho intentos para eliminar o borrar dicha información. Este residuo puede ser consecuencia de datos que quedan intactos, después de realizar una operación de eliminación de archivos, también por cambio de formato de los medios de almacenamiento, o por las propiedades físicas del medio de almacenamiento que permiten que los datos previamente escritos puedan recuperarse.[1]

Muchos factores pueden contribuir a que sea muy difícil contrarrestar la remanencia de datos, entre ellos podemos encontrar:

- ✓ Acceso al medio de almacenamiento puede tener restricciones.

[1]Remanencia de datos, http://en.wikipedia.org/wiki/Data_remanence

- ✓ Medios que puede ser casi imposible su borrado.
- ✓ Los sistemas de almacenamiento avanzados que mantienen historiales de los datos, a lo largo del ciclo de vida de los datos.
- ✓ Y por último la persistencia de los datos en memoria que por lo general se considera volátil.

La remanencia de datos puede hacer posible la divulgación inadvertida de información confidencial, si los medios de almacenamiento son liberados en un ambiente no controlado.

Varias técnicas han sido desarrolladas para solucionar esta remanencia de datos. Estas técnicas están clasificadas como, limpieza, depuración/desinfección o destrucción. Que incluyen métodos específicos como sobrescritura, desmagnetización, cifrado y destrucción física.

Existen varios estándares para la eliminación segura de los datos y la eliminación de la remanencia de datos.

III. Antecedentes

En las organizaciones, existe información que no está asociada con ningún sistema de clasificación. Esta información son a menudo copias impresas de comunicaciones internas como memorandos, informes y presentaciones. Algunas veces, esta información puede ser considerada sensible. Ejemplos de esto pueden incluir cartas disciplinarias internas, financieras o negociaciones de salario, o actas de reuniones estratégicas. Las organizaciones deben etiquetar estos medios mediante clasificaciones internas y asociar un tipo de sanitización descritos en este trabajo.

Hay diferentes tipos de saneamiento para cada tipo de medio. Se ha dividido el saneamiento de estos medios en cuatro categorías: eliminación, limpieza, depuración y destrucción. La eliminación se utiliza cuando los medios son simplemente arrojados sin darles algún tratamiento especial. Algunos medios pueden ser simplemente eliminados si la divulgación de información allí contenida no genera impacto alguno en la misión de la organización, y tampoco va a provocar daños a activos de la organización, sin dar lugar a pérdidas financieras o en daño a las personas. La eliminación es mencionada para asegurar que no todos los medios en las organizaciones requieren sanitización y que la eliminación sigue siendo un método válido para la manipulación de los medios de comunicación con información no confidencial.[2]

IV. Otros Factores a Tener en Cuenta

Al interior de las Organizaciones se deben tener en cuenta los siguientes factores:

- ¿Qué tipo y tamaño de medio de almacenamiento requiere ser esterilizado?
- ¿Cuál es el grado de confidencialidad de la información allí almacenada?
- ¿Estos medios son controlados?
- ¿Es necesario realizar este proceso con proveedores externos?
- ¿Qué cantidad de medios y de qué tipo serán sometidos a este proceso?
- ¿Cuál es la disponibilidad de equipos y herramientas para este proceso?
- ¿Qué nivel de conocimiento tiene el personal para realizar dicha acción?
- ¿Qué tiempo durará la sanitización?
- ¿Cuál sería la relación costo beneficio de llevar a cabo estos procedimientos?[3]

V. Tipos de Sanitización de Medios

Actualmente se manejan varios tipos para realizar actividades de saneamiento y eliminación de medios de almacenamiento, divididos en cuatro categorías: eliminación, limpieza, purga y destrucción, descritos en la tabla I. La eliminación es utilizada cuando el medio no tiene información relevante,

[2] Norma NIST 800-88. Tipos de sanitización pág. 7

[3] Norma NIST 800-88. Tipos de sanitización pág. 17

que pueda afectar la misión o el correcto desarrollo de las actividades dentro de la Compañía.

Se sugiere un correcto análisis de confidencialidad de la información contenida en el medio de almacenamiento, para así tomar la mejor decisión respecto al tipo de saneamiento.[4]

TABLA I
Tipos de Sanitización

Tipo	Descripción
Eliminación	Es el acto de descartar el medio sin ninguna consideración de sanitización, se realiza frecuentemente con el papel para reciclar que no contiene ningún tipo de información relevante para la organización, aunque también puede llevarse a cabo con otros medios de almacenamiento.
Borrado	Es un nivel de sanitización de medios de almacenamiento, que protege la confidencialidad de la información contra un ataque de teclado. Debe ser resistente a los intentos de recuperación de archivos por medio de utilitarios. Existen productos en el mercado tanto de software como de hardware para sobrescribir estos espacios con datos no sensibles. Este proceso puede incluir no sólo sobrescribir la parte lógica de almacenamiento, sino también la tabla de asignación de archivos. El objetivo de la seguridad del proceso de sobre escritura es remplazar los datos escritos con datos aleatorios.
Purga	Es un proceso de saneamiento de la información que protege la confidencialidad de la información contra un ataque de laboratorio. Para algunos medios de almacenamiento no es suficiente el borrado de la información, ya que mediante técnicas especiales en un ambiente controlado y con personal calificado, se podría recuperar información relevante. Se presentan ejemplos de ese proceso la ejecución del comando de borrado seguro de firmware (para drives ATA únicamente) y la desmagnetización.
Destrucción	La destrucción de los medios de almacenamiento es la última forma de saneamiento, después de que los medios de almacenamiento son destruidos, no pueden ser reutilizados. La destrucción física se puede lograr usando una variedad de métodos, incluyendo la desintegración, incineración, pulverización, trituración y fusión.

VI. Identificar la Necesidad

Es uno de los primeros pasos para tomar una decisión de sanitización de medios. No es más que analizar cuando y donde voy a necesitar la esterilización de medios que contienen información importante dentro de la Organización.

En todos los puntos de ciclos de vida de un sistema se generan elementos que contienen información, manifestados en diferentes formas, como lo pueden ser impresiones, cache de sesiones de usuarios, capturas de pantalla. El entendimiento de estas actividades permitirá a las Organizaciones identificar cuando hay necesidad de aplicar sanitización de medios y su correspondiente eliminación en caso de ser necesario.

Decisiones tan simples como colocar trituradoras de papel para eliminar medios con algún tipo de información hacen parte de esta actividad.

VII. Medios de Almacenamiento y su Reutilización

Dentro de las estrategias que deben manejar las Compañías, se debe incluir una que es la reutilización de los medios, ya sea por el tema de costos o también por el ciclo de vida de estos dispositivos, que no es más que su reciclaje después de ser sometidos a una esterilización completa.

Se valora en esta parte que hay medios que no están destinados para su reutilización y por ende se procede a su destrucción total.

VIII. Control de Medios

Una especial consideración dentro de la sanitización de medios, es su control y quien tiene acceso a estos y por ende a la información. No es lo mismo un control dentro de la Organización que un control externo. Ejemplos específicos de esto son los medios que se cambian por garantía, donde estos no serán devueltos a la Compañía.

IX. Algunas Herramientas de Software Para Realizar Sobrescritura

Dentro de los tipos de sanitización hay uno que es el borrado y dentro de este se encuentra un método que es la sobrescritura, que consiste en llenar el medio con datos no sensibles, como pueden ser ceros y unos en los espacios vacíos o donde hay información.

A continuación se mencionan diferentes soluciones de software para realizar esta actividad:

[4] Tabla tomada y traducida Norma NIST 800-88. Tipos de sanitización pág. 7 y 8

A. Harwipe

Este programa nos permite borrar de forma segura la información de un disco duro o los archivos que nosotros quisiéramos, en forma permanente, en la cual se puede utilizar alguno de los métodos de escritura de los que dispone.[5]

- **Sobrescribir en una sola pasada.** En este paso podemos elegir que sobrescriba a base de ceros o lo haga de forma aleatoria.
- **GOST R 50739-95.** Consiste en sobrescribir los datos dos veces.
- **DOD 5220.22-M(e).** Sobrescribe los datos en tres pasadas.
- **DOD 5220.22-M(d).** El mismo proceso anterior pero incluye una verificación.
- **Schneier.** Sobrescribe los datos con siete pasadas.
- **Gutmann**. Sobrescribe los datos con 35 pasadas.

Además permite tres formas diferentes de seleccionar los datos que serán sobrescritos:

- Seleccionando los archivos o carpetas directamente.
- Seleccionando el disco duro que queremos borrar completamente.
- Seleccionando el disco duro que queremos que sobrescriba sólo la zona vacía.

Al terminar el proceso presenta un informe para que se compruebe la efectividad del borrado seguro. También tiene unas funcionalidades nuevas.

- Permite, si se quiere, apagar el computador al finalizar.
- Incorpora soporte para las pantallas táctiles.
- Permite seleccionar borrado de varias unidades de disco en forma simultánea.
- Permite integración con el menú contextual del explorador de Windows.

B. Clean Disk Security

Es un programa para borrar definitivamente los datos contenidos en un disco duro, y lo hace de la única forma que es muy difícil recuperar escribiendo cada sector con ceros y unos.

Se puede configurar el número de pasadas que hará sobrescribiendo por cada sector, cuantas más pasadas, más tiempo tardará, pero más seguro será el borrado. Esta versión, permite además, borrar también, archivos temporales de Internet, documentos recientes, papelera.[6]

C. Easis Data Eraser

Permite elegir que archivos, o carpetas, que se quieren eliminar definitivamente de nuestro disco duro Además se puede elegir el nivel de seguridad del borrado.

- Podemos elegir que sobrescriba con "00″ todos los sectores del disco duro.
- También podemos decirle que haga una sobre escritura aleatoria (con un cifrado al azar) y hexadecimal 00.
- Se puede elegir el algoritmo Peter Gutmann, en el que los datos se sobrescriben 35 veces con patrones fijos y una última vez el primer bloque se sobrescribe con hex00.
- También están presentes para elegir los algoritmos de borrado, Bruce Schneier, DoD, German BSI (VS-ITR).

Por supuesto, cuanto mayor sea el nivel de borrado, más tardará el proceso pero más seguro también, y mucho más difícil será la posible recuperación.

- Prevent Restore este programa ayuda a la hora de borrar datos de forma segura en discos duros, tarjetas de memoria o pendrives, permite realizar los siguientes procesos.

[5] Borrado seguro de los datos http://cajondesastres.wordpress.com/2012/05/03/borrado-seguro-de-la-informacion-de-nuestros-discos-duros-con-hardwipe/

[6] Borrado seguro con Clean Disk Security http://cajondesastres.wordpress.com/2012/10/03/borrado-seguro-de-datos-en-el-disco-duro/

- **Display and record date of resent use**. Muestra la fecha de la última vez que se usó la aplicación.
- **Play Sound when done**. Emite una alarma sonora cuando finaliza la limpieza.
- **Prevent StandBy mode while working (WinXP only).** Impide que el equipo entre en suspension mientras está trabajando.
- **Check for Update.** Busca actualizaciones.

El aplicativo permite elegir la unidad del sistema que se quiere borrar.

- **Replace with random characters**. Rescribe los archivos con caracteres aleatorios.
- **Replace with spaces.** Rescribe los archivos con espacios en blanco.
- **Replace with random digits.** Rescribe los archivos con dígitos de forma aleatoria.
- **Yes, empty recycle bin**. Si, se quiere limpiar por completo la papelera de reciclaje.

X. MARCO CONCEPTUAL

Eliminación: es el acto de descartar o eliminar el medio sin otras consideraciones de sanitización, se realiza con más frecuencia para el reciclado de papel que no contiene información confidencial pero también puede incluir otros medios.[7]

Limpieza o borrado: es un nivel de saneamiento del medio que protege la confidencialidad de la información frente a un ataque de teclado. El simple borrado de la información no es suficiente para quitar el rastro. Esta limpieza no debe permitir recuperar los datos o emplear utilitarios de recuperación de archivos.[8]

Hay productos de software y hardware para sobrescribir el almacenamiento de los medios con datos no sensibles. Este proceso puede incluir sobre escritura, no solamente a la ubicación lógica de un archivo o archivos dentro del almacenamiento, sino también a todas las direcciones de ubicación de estos archivos.

Purga de la Información: es un proceso de sanitización de un medio que protege la confidencialidad de la información contra un ataque de laboratorio, que no es más que el uso de equipos de procesamientos de señales y personal especializado, para la recuperación de datos de un medio fuera de su entorno normal. La desmagnetización y el comando de borrado seguro del firmware del medio, son dos métodos que hacen parte del proceso de purga de información.[9]

Destrucción del medio: después de este proceso el medio no podrá ser reutilizado ya que se realiza su destrucción física, para realizar esta tarea se utilizan varios métodos como la desintegración, incineración, pulverización, trituración y fusión.[10]

Sobrescribir: Es un método común utilizado para sobrescribir los datos con otros datos, que a menudo suelen ser ceros en todas partes del medio de almacenamiento, como mínimo esto evitará la lectura de datos con solo acceder al medio.[11]

Cifrado: el cifrado de datos puede mitigar las preocupaciones que se generan sobre la remanencia de datos, ya que si la clave de descifrado es fuerte y su control es eficiente, puede hacer que la recuperación de los datos sea imposible.[12]

Áreas inaccesibles en los medios: los medios de almacenamiento pueden tener zonas que se vuelven inaccesibles, por ejemplo, los discos magnéticos pueden desarrollar nuevos sectores defectuosos después de que los datos son escritos, también las cintas requieren espacios entre registros.

Desmagnetización: es la eliminación o reducción de un campo magnético de un disco o unidad,

[7] Norma NIST 800-88. Tabla tipos de sanitización pág. 7
[8] Norma NIST 800-88. Tabla tipos de sanitización pág. 8
[9] Norma NIST 800-88. Tabla tipos de sanitización pág. 8
[10] Norma NIST 800-88. Tabla tipos de sanitización pág. 8 y 9
[11] Remanencia de Datos, http://en.wikipedia.org/wiki/Data_remanence
[12] Remanencia de Datos, http://en.wikipedia.org/wiki/Data_remanence

utilizando un dispositivo llamado degausser que ha sido diseñado para este propósito.

Sistemas de almacenamiento avanzados: aumentan la integridad de los datos mediante el registro de las operaciones de escritura en varios lugares. En tales sistemas, los restos de datos pueden existir en lugares "fuera" de la ubicación de almacenamiento de archivos nominal.

RAID: Conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usan múltiples discos duros o SSD entre los que se distribuyen o replican los datos.[13]

Fragmentación del sistema de archivos: a veces llamado el envejecimiento del sistema de archivos para disponer de datos relacionados de forma secuencial (contigua), un fenómeno inherente al almacenamiento de sistemas de archivos de copia de seguridad que permiten en el lugar la modificación de su contenido.[14]

Medios Ópticos: son medios que no son borrables porque no son magnéticos, además no pueden ser purgados por sobrescritura, CD-R, DVD-R, etc.

Borrado en FAT: En el concepto encontrado para el proceso de borrado en FAT para direcciones de archivos, se definen que son encuentran organizadas como arreglos lineales de entrada. De esta manera las entradas son valores de ciertos números de bit. Se debe tener en cuenta la versión del FAT para realizar estas entradas por ejemplo 12, 16 o 32 bit.

Cuando un archivo es borrado del contenedor, este se desvincula de la tabla del FAT la dirección del archivo y se añade un carácter especial al directorio. Indicando que está libre.[15]

Borrado en NTFS: Este proceso es muy parecido al expuesto anteriormente, ya que cuando un usuario borra un archivo este se almacena en una carpeta especial y dependiendo de la configuración del sistema operativo este será eliminado. Debido a esto el apuntador que esta direccionado al archivo también es eliminada y el cluster donde se encuentra queda disponible, además queda un registro en el log de persistencia.[16]

SSD: es un dispositivo de almacenamiento hecho con componentes electrónicos en estado sólido pensado para utilizarse en equipos informáticos en lugar de una unidad de disco duro convencional, consta de una memoria no volátil, en lugar de los platos giratorios y cabezal de las unidades de disco duro convencionales. Al no tener piezas móviles, una unidad de estado sólido reduce drásticamente el tiempo de búsqueda, latencia y otros, diferenciándose así de los discos duros.[17]

Los datos en RAM: se ha observado remanencia de datos en la memoria RAM, que por lo general se considera volátil, es decir que los contenidos se borran con la pérdida de energía eléctrica. En un estudio, se observó la retención de datos, incluso a temperatura ambiente.

Unidad USB: es un dispositivo de almacenamiento de datos que utiliza una memoria flash para guardar información, se han convertido en el sistema de transporte de datos personal más utilizado por su versatilidad, desplazando a los disquetes y a los CD.

Trituradora de papel: son aparatos que trituran documentos a trozos finos de modo que la información que contienen resulta ilegible.

Disco duro: tiene una gran capacidad de almacenamiento, en él se aloja casi toda la información cuando se trabaja en una computadora, como por ejemplo el sistema operativo que permite

[13] RAID, http://es.wikipedia.org/wiki/RAID

[14] Fragmentación del sistema de archivos, http://en.wikipedia.org/wiki/File_system_fragmentation

[15] Cano M. Jeimy J. Computación forense. Descubriendo los rastros Informáticos pág. 264 y 270

[16] Cano M. Jeimy J. Computación forense. Descubriendo los rastros Informáticos pág. 264 y 270

[17] Unidad de estado sólido, http://es.wikipedia.org/wiki/Unidad_de_estado_s%C3%B3lido

arrancar la máquina, los programas, archivos de texto, imágenes, video, etc. Dicho medio puede ser una unidad interna o fija, o externa dependiendo del lugar que ocupa en el gabinete o caja de la computadora.[18]

DRAM: (DynamicRandom Access Memory) es un tipo de tecnología de memoria RAM, es dinámica de acceso aleatorio que se usa principalmente en los módulos de memoria RAM y en otros dispositivos como memoria principal del sistema.

Fragmentación: es un problema que surge debido al ordenamiento interno de los datos en algunos sistemas de archivos. Se da muy comúnmente en el sistema operativo Windows aunque también afecta a otras plataformas pero en una escala mucho menor, también se produce fragmentación dentro de la memoria del computador (memoria RAM) cuando se asignan los procesos a los diferentes bloques de memoria. [19]

Desfragmentación: es el proceso mediante el cual se acomodan los archivos de un disco de tal manera que cada uno quede en un área continua y sin espacios sin usar entre ellos. Al irse escribiendo y borrando archivos continuamente en el disco duro, estos tienden a no quedar en áreas contiguas, un archivo puede quedar "partido" en muchos pedazos a lo largo del disco, se dice entonces que el archivo está "fragmentado".

Sistema Operativo: es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.[20]

WINDOWS: Nombre de una familia de sistemas operativos desarrollados y vendidos por MICROSOFT, está basado en ventanas y es el más utilizado a nivel mundial.

LINUX: es un sistema operativo cuyo desarrollo es uno de los ejemplos más prominentes de software libre; todo su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (General PublicLicense), puede funcionar tanto en entorno gráfico como en modo consola.[21]

Método GUTMANN: Es un algoritmo para borrar con seguridad el contenido de los discos duros de un ordenador, como los archivos. Ideado por Peter Gutmann y ColinPlumb.

XI. CONCLUSIONES

Las Organizaciones deben prestar más atención a estas consideraciones y diseñar estrategias para manejar el tema de la sanitización de medios, ya que es algo fundamental en el manejo de la información.

El uso de herramientas confiables y eficientes en la sanitización de los medios permite el aseguramiento del flujo de la información.

REFERENCIAS

[1] CANO MARTINEZ. Jeimy J. Computación Forense. Descubriendo los Rastros Informáticos. México, Editorial Alfaomega S.A. 1ª edición.
[2] COSTA S. Jesús. Seguridad Informática. México Editorial RA-MA.
[3] Disponible en internet: glu.unicauca.edu.co/wiki/aimages/1/1d/InfoForense.pdf
[4] Informática Forense: http://www.acis.org.co/fileadmin/Conferencias/BorradoSeguro.pdf
[5] Computo Forense: http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Herramientas_para_el_an.C3.A1lisis_de_discos_duros

Autores
Carlos Javier Osorio Beltrán, Ingeniero de Sistemas.

[18] Dispositivo de almacenamiento de datos, https://es.wikipedia.org/wiki/Dispositivo_de_almacenamiento
[19] Desfragmentación, http://es.wikipedia.org/wiki/Desfragmentaci%C3%B3n
[20] Sistema Operativo, http://es.wikipedia.org/wiki/Sistema_operativo
[21] GNU/Linux, http://es.wikipedia.org/wiki/GNU/Linux

Alexander Calderón, Ingeniero de Sistemas.