BORRADO SEGURO DE LA INFORMACIÓN PARA LA DONACIÓN DE EQUIPOS OBSOLETOS

Bernal Macías, Juan Gabriel
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia
Jaun88@msn.com

Resumen- En este artículo se evidencia la importancia de realizar un borrado seguro de la información en equipos obsoletos, dañados y dispositivos de almacenamiento, los cuales pueden contener información de organizaciones o personas en particular. Estos son donados a fundaciones y otras empresas que determinan su disposición final, por esta razón se ha de realizar una recopilación bibliográfica de los principales antecedentes, métodos e información relevante del borrado seguro de la información, que ayuden a determinar los riesgos vitales a los que se exponen. A través de esta revisión se podrán establecer políticas para implementar métodos para el borrado seguro de la información.

Palabras Clave: Borrado seguro de información, almacenamiento, recuperación, eliminación, donación, reciclaje, vulnerabilidad, riesgo, amenaza, activos, impactos.

Abstract- This article highlights the importance of performing secure deletion of information stored by companies Cooperative sector hard drives to computer equipment donated voluntarily surrender or recycling to third parties. For this reason, it has to make a bibliography of the main background, methods and relevant information secure deletion of information to help determine the critical risks to which they are exposed. Through this review, we will develop policies to identify how efficient and safe methods employ techniques for erasing this information.

Index Terms: Secure deletion of information, storage, retrieval, disposal, donating, recycling, vulnerability, risk, threat, assets, and impacts.

I. INTRODUCCIÓN

En la actualidad la tecnología avanza a pasos gigantescos, a tal punto que cuando se adquiere un nuevo equipo de cómputo, al mes ya ha salido una nueva referencia con mejores componentes y más potencia que la adquirida. Día a día los desarrolladores de software implementan programas, bases de datos y otras aplicaciones, que requieren equipos más robustos para minimizar los tiempos que tardan los procesos y mejorar la calidad que el usuario final requiere.

Esto nos lleva a la conclusión que los equipos pierden valor en menos tiempo, teniendo así que destinar un uso final para ellos. Actualmente a las organizaciones se les brinda múltiples opciones con grandes beneficios, una de ellas la buena disposición de desechos tecnológicos a entidades de reciclaje los cuales certifican este proceso con un acta, esto ayuda a minimizar los impuestos de la organización, otra opción es donar los computadores para educación a escuelas o fundaciones, lo cual brinda el mismo beneficio.

En la actualidad, la información se ha vuelto el activo más importante de las organizaciones por lo tanto, los medios de almacenamiento en los que se encuentran estos activos representan un alto riesgo ya que es muy común que las maquinas sean entregadas sin eliminar la información de forma segura.

Al realizar este proceso, se debe quitar todo tipo de información y registros que pueda contener el disco duro, ya que el activo más valioso de una organización es la información y esta no puede caer en manos de terceros. Este proyecto propone evitar la fuga de información al entregar equipos por obsolescencia a diversas entidades, mediante una técnica para conservar la confidencialidad e integridad de la información.

La Norma ISO 27001 está basada en la seguridad de la información, sus pilares fundamentales consisten en la confidencialidad, la disponibilidad y la integridad de la información, además de ser una norma es gestión de seguridad de la información. [1].

A. Disponibilidad

Consiste en mantener al alcance de la mano algo que se necesita constantemente o de forma continua, como el correo.

B. Confidencialidad

Es un ámbito en el cual se garantiza que la información esté disponible únicamente a personal autorizado.

C. Integridad de los datos

La integridad hace referencia a los valores reales de la información los cuales son utilizados en aplicaciones o bases de datos.

II. LA IMPORTANCIA DEL BORRADO SEGURO DE LA INFORMACIÓN

Las entidades que año tras año desechan equipos de cómputo, no perciben el alto riesgo al que exponen su activo (la información), este riesgo avanza de manera acelerada al igual que la tecnología.

Evidentemente con los avances de la tecnología, también evoluciona el conocimiento de las personas, al darse este hecho, se hace más fácil extraer de los ordenadores información confidencial, la cual puede ser adquirida por competidores o antiguos empleados para ser aprovechados en perjuicio de las organizaciones o personas en particular.

Para algunas entidades el riesgo puede llegar a ser más alto que para otras, esto depende de su actividad económica y la cantidad de información que manejan como millones de datos personales o varios datos que al ser desechados sin ninguna política de borrado permite extraer con facilidad la información mediante procedimientos de recuperación [2]. En términos legales, se estaría infringiendo la ley 1581 de 2012, la cual regula la protección de datos personales, que se encuentran en cualquier tipo de entidad, donde se maneje una base de datos o una base social, de información también se estaría infringiendo el Artículo 15 de la Constitución Política de Colombia, el cual contempla el derecho de todo ciudadano colombiano a tener intimidad, estas leyes se deben tener en cuenta para desarrollar políticas de borrado seguro.

El procedimiento de borrado es una acción que hace el usuario para eliminar un archivo que no se necesita, desde otra vista técnica es una acción que marca unos sectores del disco como libres así no lo sean; este es un borrado común no implica que el disco tenga los sectores libres haciendo que estén disponibles para sobre escribirlos. El borrado seguro es más profundo porque trata de hacer un cambio en la combinación del archivo, este procedimiento debe realizarse por determinadas maneras para cumplir con el objetivo de borrado seguro y que no se pueda recuperar el archivo.

En el formateo de un dispositivo de almacenamiento podemos ver que una cantidad o el total de la capacidad está libre pero esto no es así, todos los archivos antes guardados están intactos por lo que se podrán recuperar por partes con procedimientos y software de recuperación. Actualmente en las empresas y entidades públicas se cree que utilizan medidas de borrado seguro pero no son los suficientemente eficientes al no realizar el borrado seguro con software o métodos que cambien los valores de la información guardada, esto implica que ponemos en riesgo la información de clientes, proveedores, empleados e información confidencial de la empresa que puede ser la estructura de funcionamiento, uno de los ejemplos que vemos continuamente son los desechos tecnológicos, reciclaje electrónico o reventa; los dispositivos se entregan a terceros, y los elementos de almacenamientos o equipos completos que no han pasado por un proceso de borrado seguro, pueden caer en manos equivocadas poniendo en riesgo dicha información; por esta razón es necesario tomar las medidas adecuadas para evitar que existan fallas en las técnicas de eliminación de la información y que esta sea realmente eliminada de forma segura, esto lo podemos hacer mediante políticas definidas que indiquen que procesos seguir cuando un equipo sea para cambio o desecho lo que conlleva asegurar que se realiza el proceso de borrado seguro. Para evitar que la información sea divulgada o utilizada por terceros se debe poner en práctica las políticas de borrado seguro no solo al momento de desechar un disco si no también se

debe realizar esto cuando un usuario común desea eliminar un archivo que no utilizará más; para esto podemos encontrar diversas aplicaciones que nos ayuda a eliminar de forma definitiva y sin riesgos la información.

III. OBJETIVO DEL BORRADO

El objetivo del documento es identificar las políticas o procesos que ayudan a establecer un modo eficiente para la eliminación o destrucción de archivos confidenciales basados en técnicas que permitan el borrado seguro de la información en dispositivos que han sido utilizados, cambiados o que vayan hacer reciclados, de esta manera analizar los antecedentes que se han manipulado para identificar los método más eficientes de destrucción de archivos. Este objetivo requiere análisis de los antecedentes de eliminación de archivos o procesos de borrado para construir técnicas orientadas a la identificación y planeación para realizar un borrado seguro cuando un dispositivo de almacenamiento sea reciclado, de esta manera se identifican las vulnerabilidades en el proceso de borrado, de acuerdo a esto construir un método de eliminación y así una política que se pueda implementar en una empresa e incrementar los niveles de seguridad de la información.

La implementación de políticas para cada empresa es diferente por la naturaleza de cada negocio, por lo cual se deben catalogar adecuadamente las vulnerabilidades más importantes, de forma que se genere un protocolo que garantice que la información contenida en dispositivos como discos duros sea destruida antes de ser reciclada, desechada o vendida nuevamente, permitiendo brindar seguridad y confianza a las organizaciones, de esta manera se podrán implementar planes de acción para mitigar los riesgos de la información.

Utilizar políticas de seguridad o buenas prácticas de borrado seguro certificará los cumplimientos legales de no divulgación de datos personales cumpliendo así con las normas vigentes legales y de buen manejo de la información según la ISO2701 que certifica esto.

IV. ALCANCE

La importancia de este documento está ubicado en la línea de prevención del riesgo, buenas prácticas de ITIL la cual está alineada con la norma ISO 27001 en informática, en el que se enmarcan temas para establecer las políticas de seguridad basadas en las vulnerabilidades de la información de los dispositivos de almacenamiento, se debe tener en cuenta algunos pasos fundamentales para erradicar los procesos erróneos que vemos en algunas empresas que desechan dispositivos de almacenamiento, estos son:

- Identificación del proceso actual.
- Métodos de borrado seguro.
- Verificación de la no restauración de los archivos, después del borrado seguro establecido.
- Implementación de las políticas de borrado seguro.

V. BORRADO SEGURO DE LA INFORMACIÓN

En empresas privadas y públicas manejan información que es almacenada en los ordenadores y esta incrementa con el tiempo y modo de uso por lo cual aumenta todos los días dado a esto la información es traslada o emitida a otros usuarios que necesitan su contenido para hacer una acción que conlleva a otros aspectos actualmente los sistemas operativos como Microsoft Windows que es el más utilizado no muestra una interfaz amable y agradable para trabajar y realizar labores cotidianas de cualquier trabajo está interfaz muestra una papelera de reciclaje que utilizan usuarios comunes pero que no están teniendo en cuenta la importancia de los archivos y riesgos que tendrían si la información estuviera en manos de terceros. Desde este punto de vista vemos que necesitamos hacer una cultura de importancia del flujo de información que se maneja en una empresa para los empleados que aún no son conscientes de la información que tiene a su disposición por lo cual si implementamos las políticas de borrado seguro ayudaremos a concientizar a los usuarios de la información, también podemos utilizar herramientas o software que les permitan hacer un borrado totalmente seguro. Para esto se debe indagar sobre los dispositivos que se utilizan para

el almacenamiento y así se establece cuáles son los pasos a seguir:

A. Almacenamiento

Se debe hacer una clasificación de la información que se está almacenando, no toda la información es sensible o tiene una criticidad alta de acuerdo esto lo define el usuario el que será encardo de actualizar el dispositivo de almacenamiento.

B. Borrado Seguro

Para asegurar que el borrado sea seguro podemos utilizar software que nos permite cambiar los valores del archivo volviéndolos irrecuperables lo cual sucederá cuando el usuario de por concluida su vida útil.

C. Recuperación

Se deben emplear varias técnicas de recuperación de archivos para asegura que los archivos no se puedan recuperar para prevenir la perdida por errores humanos o de maquina es importante contar con un respaldo de la información la cual puede estar en un servidor de copias de respaldo, lo que garantiza el correcto manejo de información.

VI. POLÍTICAS DE ALMACENAMIENTO EN RED

Es necesario identificar la información de la empresa la que manejan los usuarios e información de los empleados la cual debe estar guardada en la red corporativa, ésta debe tener un funcionamiento de uso compartido para que el usuario la puede consultar y utilizar cuando lo necesite, la cual tendrá ciertos controles que son definidos por el administrador de la red. Los empleados también pueden disponer de carpetas compartidas en red a las cuales tiene acceso solo el usuario especifico que puede ingresar y consultar la información allí almacenada por esto es importante concientizar a los empleados de que los archivos deben de tener una vida útil y que deben ser borrados mediante el proceso seguro también este proceso se debe realizar en las unidades de almacenamiento local según los criterios de almacenamiento antes vistos. De esta manera se encuentran dos tipos de información.

A. Información de los empleados

La información de los empleados es aquella que la puede tener disponible en el correo en las unidades de almacenamiento local o en red corporativa esta información es de uso clasificado es decir que solo un grupo limitado de empleados puede tener acceso o conocimiento de los archivos. Los archivos que pueden contener información estructural de la empresa la cual estará actualizándose según sea el modelo de negocio por esta razón es parte fundamental de la seguridad de la información que no esté en las manos de terceros.

B. Información de la empresa

La información de la empresa es aquella que contiene aspectos legales bancarios y datos personales de los empleados por lo cual es de alta importancia que esta información no esté en manos equivocadas. Esta información debe manejarse con factores de seguridad ya que no los puede manejar cualquier tipo de usuario esta información se puede duplicar en la red por medio de correos carpetas compartidas y dispositivos de almacenamiento local esto genera incertidumbre de la información por ello esto debe estar guardado en dispositivos de almacenamiento en red.

VII. DESTRUCCIÓN DE LA INFORMACIÓN

Para completar el ciclo de vida de la información en cuanto a la seguridad, es preciso cubrir un aspecto de suma importancia como es la destrucción de la información. Las empresas pueden encontrar diversos motivos para eliminar la información que guardan pero siempre tiene un ciclo de vida lo que conlleva a una destrucción final. Además las áreas de TIC (tecnologías de la información y comunicación), son las encargadas de la adecuada gestión de datos personales, estratégicos, legales o contables, entre otros, y están obligadas a conservar estos datos durante un periodo de tiempo, tras el cual se suelen eliminar de forma permanente. Por esta razón es necesario analizar la información que información será destruida y que usuarios pueden tenerla. Desacuerdo a esto veremos los métodos de destrucción.

A. Desmagnetización

Consiste en la alteración de los soportes de almacenamiento cuando un campo magnético

como un imán es utilizado sobre un disco ocasiona una polarización de las partículas y de esta forma un borrado seguro esto se debe de hacer según el tamaño físico del disco por lo cual varia la potencia del medio magnético que tenemos que emplear. Tras el proceso es de comprender que el disco o medio de almacenamiento dejara de funcionar correctamente y tiene que ser remplazado para evitar la pérdida de información por error de maquina este es uno de los procesos que se es más utilizado para que la destrucción de la información de manera segura.

B. Destrucción física.

La destrucción física es la invalidación del medio de almacenamiento para evitar la recuperación de la información almacenada, actualmente hay dos procedimientos de destrucción física.

C. Trituración

Es un procedimiento en el cual se destruye de forma física el disco dependiendo el tamaño será aplastado y desintegrado.

D. Desintegración

Este es el más común utilizado y se realiza por medio de una destructora de metal o una plata de inserción que es la forma más eficaz y segura de realizar este procedimiento indispensable.

VIII. RIESGOS ASOCIADOS

Actualmente es muy fácil adquirir nuevos archivos y crear otros con información lo cual ocurre simplemente al descargar una base de datos y estos son eliminados constantemente sin conciencia de que esta información puede ser extraída los riesgos se tiene que mitigar desde el usuario con la clasificación de los archivos y software que le permita eliminar lo que el considere como inutilizable; el segundo nivel es del área de soporte la cual tiene que realizar el borrado seguro mediante los pasos o metodología estructurada en las políticas de seguridad más sin embargo existen riesgos los cuales deberían ser depurados con los métodos de destrucción de la información antes mencionados.

Como se ha indicado anteriormente los métodos que algunas empresas utilizan actualmente es un simple formateo o borrado de la información pero estos son las técnicas inapropiadas para la depuración de la información esto hace que en el momento que los dispositivos de almacenamiento sean desechados reciclados o vendidos con técnicas de recuperación o con simple software de recuperación sea extraída la información. Las empresas ignoran esto o especulan que al borrar simplemente los archivos o que al formatear un disco la información es irrecuperable. Esto puede causar afectaciones a la entidad en varios ámbitos, tanto financieros como a su imagen los riesgos asociados al robo de identidad tales como fugas de información corporativa, filtrado de información confidencial de clientes e innumerables problemas que están asociados al dar de baja computadoras, servidores, equipos de almacenamiento o de respaldo y muchos otros dispositivos que no utilizan un apropiado método de borrado seguro. El borrado seguro de información permite minimizar estos riesgos y asegura que la información que alguna vez estuvo en los dispositivos desechados reciclados o reacondicionados desaparezca totalmente pese a cualquier posible intento de ser recuperados. A continuación se explicara algunos métodos de eliminación segura como buen manejo de la información en medios magnéticos.

IX. MÉTODOS DE ELIMINACIÓN SEGURA

A continuación se realiza una breve muestra de los diferentes métodos de borrado seguro de información en discos duros utilizados actualmente a nivel mundial.

A. American DoD 5220-22M Standard Wipe

Norma a nivel gobierno en Estados Unidos. Este método consiste en la sobre escritura del soporte con un valor fijo determinado una vez (ejemplo 0x00) y a continuación se escribe su valor complementario (0xff) una vez y finalmente se repasa con valores aleatorios una vez. Al verificar el disco se puede comprobar la escritura correcta de los valores. Usualmente se utiliza con tres sobre escrituras con tres verificaciones. Está clasificada con grado 10, considerado con nivel de seguridad medio.

C. Canadian RCMP TSSIT OPS-II Standard Wipe

Este estándar cuenta con siete sobre escrituras y siete verificaciones, es implementado por "Royal Canadian Mounted Police" y TSSIT con "Technical Security Standard for Information Tecnology" además de otras entidades gubernamentales. Tiene clasificación grado 12 y nivel de seguridad Medio.

D. Pseudo random data

Emplea el algoritmo ISAAC (Indirection, Shift, Accumulate, Add and Count) este es un generador pseudoaleatotio de número (PRNG) además de un cifrador de flujo de Bob Jenkins, que es el que le da el nombre al generador, la característica más importante de este estándar es que permite al usuario seleccionar el número de pasadas para sobre escritura con un máximo de 65535. Ya que los datos son aleatorios son altamente incomprimibles, es uno de los métodos que requiere ser usado en unidades comprimidas. Su clasificación es grado 11. Nivel de seguridad: Medio.

E. North Atlantic Treaty Organization-NATO standard

Este es el estándar de borrado de la OTAN (North Atlantic Treaty Organization), permite la sobre escritura del soporte siete veces. Las primeras seis pasadas son de sobre escritura con valores fijos que son alternativos entre cada pasada (0x00) y (0xff). La séptima y última pasada sobre escribe con un valor aleatorio. Cuenta con una clasificación grado 12. Su nivel de seguridad es: Alto.

F. Método Gutmann

Emplea el algoritmo ISAAC para pasadas adicionales con datos aleatorios antes y después de escribir las propias 27 del método Gutmann, es decir la sobre escritura de este soporte se realiza grabando valores aleatorios sobre cada sector. A continuación se sobrescribe todo el soporte en valores pseudo aleatorios sobre cada sector durante veintisiete pasadas (esto se conoce como patrón 531). Para finalizar, se escriben valores aleatorios durante cuatro pasadas en cada sector (cuatro patrones). Para un total de treinta y cinco pasadas de sobre escritura, es decir treinta y cinco patrones [3].

Destrucción Física	Desmagnetización	Sobre-escritura
✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información	✓ Eliminación de forma segura de la información
✗ Un sistema de destrucción para cada soporte	✗ Una configuración del sistema para cada soporte	✓ Una única solución para todos los dispositivos
✗ Dificultad de certificación del proceso	✗ Dificultad de certificación del proceso	✓ Garantía documental de la operación
✗ Necesidad de transportar los equipos a una ubicación externa	✗ Necesidad de transportar los equipos a una ubicación externa	✓ Posibilidad de eliminación en las propias oficinas
✗ Medidas extraordinarias para garantizar la cadena de custodia	✗ Medidas extraordinarias para garantizar la cadena de custodia	✓ Garantía de la cadena de custodia
✓ Destrucción de dispositivos, no Regrabables, ópticos	✗ Sólo válido para dispositivos de almacenamiento magnético	✗ No válido para dispositivos no regrabables ni ópticos
✗ Destrucción definitiva y dificultad de reciclaje de materiales	✗ Tras el proceso el dispositivo deja de funcionar correctamente	✓ Reutilización de los dispositivos con garantías de funcionamiento

Fig.2. Comparativa de los métodos de borrado seguro[1]

X. POBLACIÓN

El documento estará orientado a los dispositivos de equipos en reciclaje reutilización y desechos por motivos de obsolescencia, tecnológica y renovación de tecnología.

XI. ETAPAS

Al tomar una muestra de alguna compañía se tendrá en cuenta la siguiente secuencia de eventos, dividida por etapas.

A. Etapa de recolección de información

Para la recolección de información se tiene previsto un acuerdo con empresas que trabajan con reciclaje electrónico como PCSHEK, que es una empresa que reutiliza los desechos tecnológicos por medio de la destrucción, lo que quiere decir es que de algunos discos desechados se tratará de recuperar la información.

B. Etapa de Pruebas

Se aplicaran los distintos métodos de borrado seguro existentes para determinar su efectividad, metodología y eficacia, para así concluir cual es la mejor herramienta para realizar el borrado seguro.

C. Etapa 3 de análisis de la información

A partir de los resultados obtenidos en la realización de las pruebas, se deben crear

[1] Vjavierf.wordexpress.com. Borrado seguro de la información. [En línea].12 de mayo de 2012. Disponible en https://vjavierf.wordpress.com/2011/05/12/borrado-seguro-de-la-informacion/

metodologías más enfocadas y políticas de seguridad de borrado seguro.

XII. RESULTADOS ESPERADOS

Se espera obtener con el progreso de este borrado seguro lo siguientes:

• Reducción riesgos al utilizar metodologías de filtración de información.

• Metodologías de los procesos de borrados realizados, para seleccionar una herramienta que nos indique o que nos muestre un informe de los elementos borrados.

• Confidencialidad de los datos borrados al implantar una política o pasos para el borrado seguro.

• Creación de políticas de seguridad que permitan el borrado seguro de la información y óptimo de un disco duro.

• Revisión de los diferentes métodos de borrado seguro existentes en el mercado y adoptar un método óptimo que minimice costos, tiempo y ofrezca seguridad.

REFERENCIAS

[1] P. Aguilera," Seguridad informática". Editor Editex, 2010. 240 pp. ISBN: 9788497717618.

[2] Cryptex – Seguridad de la Información. Herramientas y Métodos de Borrado Seguro. [En línea]. Mayo 28 de 2008. Disponible en http://seguridad-informacion.blogspot.com/2008/05/herramientas-de-borrado-seguro.html

[3] Academia. RITS 3 Informática Forense. [En línea]. 2009. Disponible en http://www.academia.edu/4288731/RITS_3_INFORMATICA_FORENSE

Autor

Juan Gabriel Bernal Macías. Nació en Bogotá D.C. en 1988. Recibió el título de Ingeniero de Sistemas de la Universidad Piloto de Colombia en el año 2011 Desde el año 2010 al 2012 laboró en el Banco BBVA como Analista de Seguridad e Infraestructura. Actualmente se desempeña como Administrador de Infraestructura en Coopetrol y realiza estudios de Postgrado en Seguridad Informática en la Universidad Piloto de Colombia.