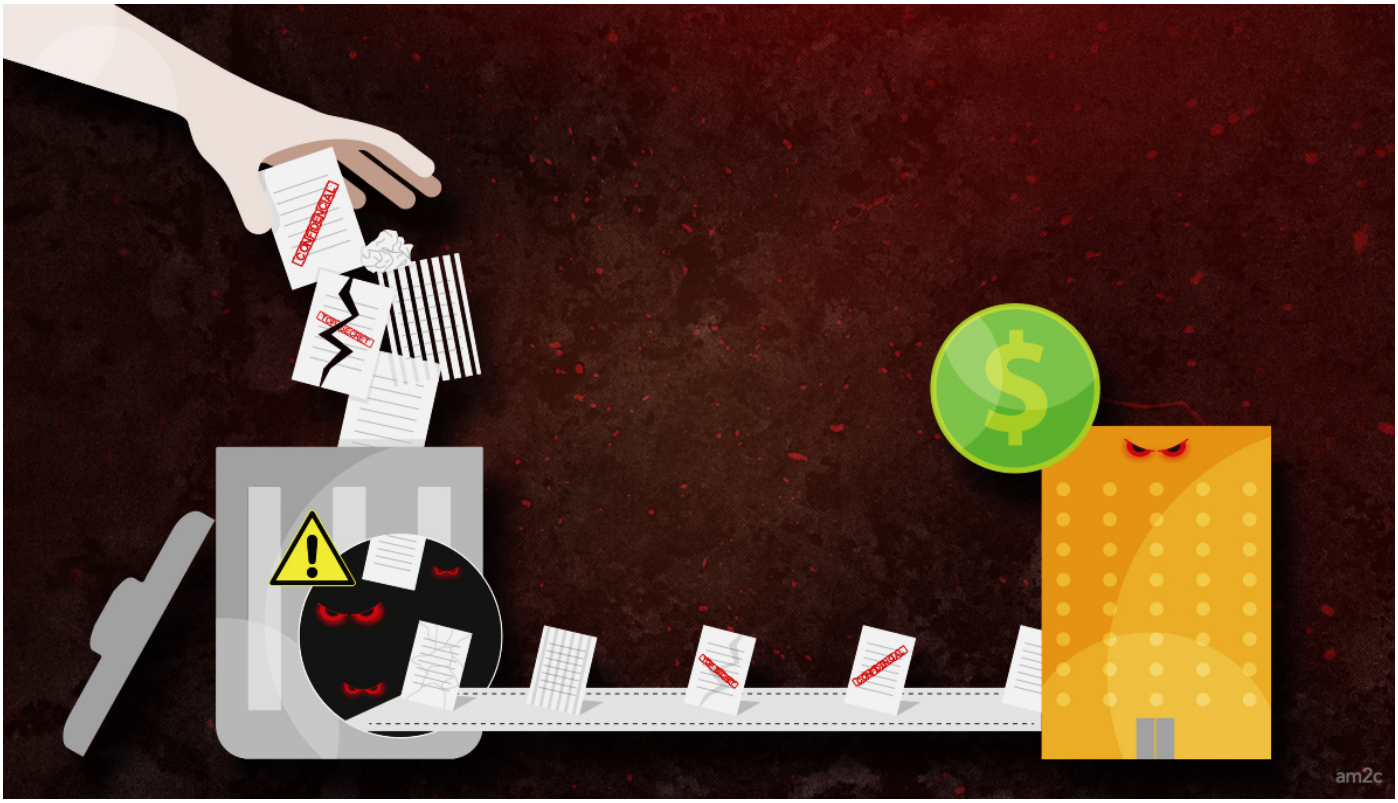
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

SANITIZACIÓN DE INFORMACIÓN

Edgar Ríos Clemente

sanitización

numero-28



La información es uno de los activos más importantes de las organizaciones. Durante su ciclo de vida debe ser protegida mediante diversos controles de acuerdo a su estado (en reposo, en tránsito o en uso). Una vez que finaliza su ciclo de vida, se debe contar con procesos de destrucción segura para que dicha información no pueda ser reutilizada con otros fines.

Uno de los pasos que hay que tomar en cuenta cuando un dispositivo o la información que contiene deja de ser útil, es realizar una eliminación de manera segura.

La sanitización de datos, de acuerdo con el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés), se refiere a un proceso que no permite el acceso a los datos sobre los medios para un determinado nivel de esfuerzo, es decir, que los datos no se recuperen fácilmente.

RIESGOS DE NO SANITIZAR LOS DATOS

Cuando la información no es eliminada de forma segura, la información importante puede remanecer, lo cual puede derivar en probables riesgos como:

- Datos privados o personales de los clientes o empleados pueden ser utilizados para cometer fraude o robo de identidad.
- Datos críticos pueden ser recuperados y usados por adversarios o competidores.
- Fuga de datos privados o personales que deriven en grandes multas y acciones legales para las organizaciones, por no cumplir con las leyes de protección de datos personales.

- La propiedad intelectual puede ser recuperada y publicada, derivando en pérdida de reputación y/o ganancias.

La **clasificación** contribuye en la valuación y protección de los activos de información; esto incluye también los procesos y procedimientos para reclasificarla, porque después de un periodo la información considerada como sensible puede declinar en valor o criticidad (de esta forma se evita que haya controles de protección excesivos). Por lo anterior, dentro de las políticas de clasificación de información, deberá también incluirse la reclasificación de información física y digital.

Por otra parte, en México el robo de identidad es un tema importante. Según datos del Banco de México, nuestro país ocupó en 2015 el octavo lugar a nivel mundial en este delito; debido a esto, como una medida de control, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha creado una guía completa para prevenir el robo de identidad, la cual se puede consultar en el siguiente enlace, que hace referencia a métodos para sanitizar la información.

MOTIVOS PARA SANITIZAR

Algunas de las razones por las que se requiere sanitizar los medios de almacenamiento son:

- **Reutilizar**: Cuando se quiere reubicar el dispositivo a un usuario diferente o utilizarlo con otro propósito.
- **Revender**: Cuando se quiere revender el dispositivo y ya cuenta con nuestros datos personales, principalmente si son identificables.
- **Reparar**: Cuando se tiene que llevar a reparación, pero ya cuenta con información personal delicada.
- **Eliminar**: Al desechar o al donarlo, dar de baja el dispositivo.
- **Destruir**: Cuando se cuenta con información confidencial, la cual requiere que sean destruidos físicamente los dispositivos.
- **Regulatorio**: Por cumplimiento de regulaciones como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) o la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Actualmente existen diversas organizaciones que cuentan con programas de donación o reciclaje de dispositivos electrónicos que incluyen celulares, computadoras portátiles, servidores, consolas de videojuegos y tabletas.

Empresas como Microsoft sugieren contactar a sus socios comerciales para apoyarse en la eliminación de información personal identificable; desafortunadamente, en México no se cuenta con *partners* que realicen este servicio de acuerdo con su sitio web pero, por otra parte, existen empresas nacionales que realizan esta labor.

En el país, los servicios más comunes que se ofrecen para la destrucción física de los documentos y los dispositivos físicos (discos magnéticos) son la desmagnetización, la trituración y la incineración.

ADMINISTRANDO LOS RIESGOS DE MEDIOS DE ALMACENAMIENTO

Para contar con un mejor manejo de riesgos asociados con el almacenamiento de información sensitiva, el Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés) del Reino Unido recomienda:

- Entender los datos y su valor potencial fuera de la organización.
- Comprender el costo de la sanitización de la información y añadirlo a los costos de adquisiciones para asignar un presupuesto.
- Contar con una política de reutilización y eliminación, con roles clave entendidos por todos en la organización.
- Conocer las tecnologías que se están empleando.

- Conservar los manuales de fabricantes para conocer cómo desechar y sanitizar.
- Establecer el ciclo de vida del medio de almacenamiento (qué se almacena, dónde y por cuánto tiempo).
- Usar terceros confiables que se apeguen a estándares internacionales.
- Obtener certificados de destrucción de los servicios de terceros (algunos proveedores adicionalmente proporcionan el video de la destrucción).
- Supervisar que los procesos de destrucción y equipo son probados periódicamente.
- Verificar que los datos son sanitizados apropiadamente.
- Remover las etiquetas o marcas indicando pertenencia del dispositivo o de los datos contenidos.
- Clasificar y etiquetar la información para que tenga el proceso adecuado y reducir posibles fugas o pérdidas.

Debido a estos escenarios, se requiere el uso de diferentes tecnologías y/o métodos para que se elimine la información de forma segura.

ESTÁNDARES DE SANITIZACIÓN Y DESTRUCCIÓN DE DATOS

El Reino Unido cuenta con el estándar Her Majesty's Government (HMG) Infosec Stardard 5 (IS5) para destrucción de datos; en Europa se tiene el estándar de destrucción de la información EN15713; en Alemania cuentan con el estándar DIN-66399; mientras que en los Estados Unidos de América se pueden seguir las guías de sanitización de medios del Instituto Nacional de Estándares y Tecnología NIST-800-88.

En México aún no contamos con una norma o estándar, pero una propuesta es la guía para el Borrado Seguro de Datos Personales desarrollada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), la cual es muy completa.

Actualmente, las organizaciones líderes de ciberseguridad, como el NIST, ya no cuentan con una lista de herramientas aprobadas, tal vez debido a la existencia de métodos más sofisticados para recuperación de información, al grado de que ya no es recomendable únicamente la sobreescritura en los discos magnéticos (aunque en la práctica es mejor siempre hacerlo). Sin embargo, el equipo de ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) cuenta con un catálogo de productos para eliminación de discos magnéticos que puede ser de utilidad cuando se buscan opciones de eliminación más robustas.

CONCLUSIONES

Los medios de almacenamiento evolucionan muy rápido, por lo cual habrá que identificar las nuevas tecnologías y los métodos de sanitización de datos más actuales para proteger los datos de las organizaciones.

Es importante mencionar que el contar con los procesos y el presupuesto para la sanitización de

información ayudará a administrar diversos riesgos asociados a la falta de protección de información, sin olvidar que deben ir de la mano con las políticas de clasificación y retención de información. Por esta razón, se han mencionado en el artículo diversos estándares internacionales, así como las mejores prácticas nacionales. De esta forma, los encargados de proteger la información pueden apoyarse en ellos para la generación de políticas, procesos y estándares que mejor se adapten a las necesidades de cada organización.

Es importante que al finalizar el ciclo de vida de la información, se aplique alguna (o varias) de las técnicas de sanitización de datos, de acuerdo con el tipo de información. De este modo se minimizará el riesgo de que dicha información sea reutilizada con otros fines.

Para organizaciones que requieran contratar servicios de destrucción de datos (incluyendo medios magnéticos e información física) en el país, una opción es elegir una empresa que pertenezca a una asociación internacional como la National Association for Information Destruction (NAID) de los Estados Unidos de América.

REFERENCIAS

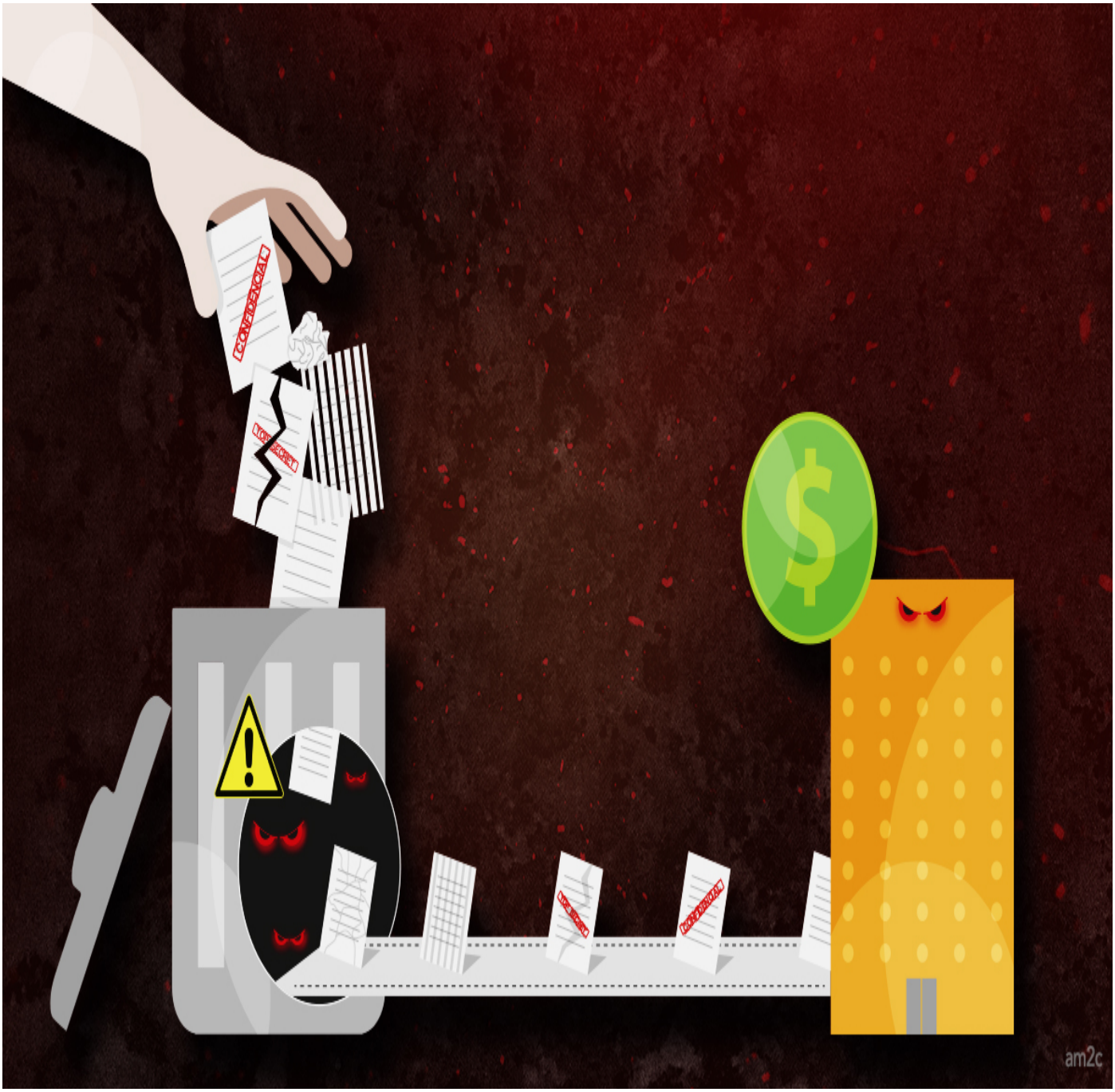
- Arch Linux. (13 de noviembre de 2016). Securely wipe disk. *Arch Linux.* Recuperado de: https://wiki.archlinux.org/index.php/Securely_wipe_disk
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (Junio de 2016). *Guía para el Borrado Seguro de Datos Personales.* Recuperado de: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf
- ————. (2016). *Guía para Prevenir el Robo de Identidad.* Recuperado de: http://inicio.inai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf
- Microsoft. (2017). How to more safely dispose of computers and other devices. *Microsoft.* Recuperado de: https://www.microsoft.com/en-us/safety/online-privacy/safely-dispose-computers-and-devices.aspx
- National Cyber Security Centre. (24 de septiembre de 2016). Secure sanitisation of storage media. *Guidance.* Recuperado de: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- National Institute of Standards and Technology. (Diciembre 2014). *Guidelines for Media Sanitization*. Recuperado de: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- North Atlantic Treaty Organization. (2014). Disk Erasure. *Information Assurance Product Catalogue*. Recuperado de: http://www.ia.nato.int/niapc/Category/Disk-Erasure_11
- Rothke, B. (24 de febrero de 2009). Why Information Must Be Destroyed. *CSO.* Recuperado de: http://www.csoonline.com/article/2123705/privacy/why-information-must-be-destroyed.html
- ————. (5 de mayo de 2009). Why Information Must Be Destroyed, Part Two. *CSO.* Recuperado de: http://www.csoonline.com/article/2123985/data-protection/why-information-must-be-destroyed--part-two.html

- Wikipedia. (26 de marzo de 2017). Persistencia de datos. *Wikipedia.* Recuperado de: https://es.wikipedia.org/wiki/Persistencia_de_datos
- ————————. (19 de noviembre de 2016). Sanitización de datos. *Wikipedia*. Recuperado de: https://es.wikipedia.org/wiki/Sanitizaci%C3%B3n

SI QUIERES SABER MÁS:

- Guía de sanitización segura de medios de almacenamiento del Centro Nacional de CiberSeguridad del Reino Unido (NCSC)
- Guía para el Borrado Seguro de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
- Guía de destrucción de información EN15713:2009 de la british security industry association (BSIA)
- Directrices para sanitización de medios del Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América (NIST)

Imagenes adjuntas:


CONFIDENTIAL
CONFIDENTIAL
CONFIDENTIAL
am2c

Source URL: http://revista.seguridad.unam.mx/numero28/sanitizacion-de-informacion