Delete Technology

Powered by blancco

LOS CENTROS CRIPTOLÓGICOS GLOBALES Y SUS ESTÁNADRES DE CIBERSEGURIDAD

Delete Technology Group

Objetivo

Un artículo sobre el papel de los Centros Criptológicos en la seguridad e investigación en contextos gubernamentales y en el que se abordan los sistemas y estándares de ciberseguridad de Alemania, Reino Unido, Estados Unidos, Japón, Canadá y la OTAN.

¿Qué son los Centros Criptológicos y cuál es su papel en la seguridad de los datos?

Los Centros Criptológicos son los entes responsables de la evaluación y certificación de productos y servicios criptográficos. Esto incluye la evaluación de la seguridad de los productos y la investigación, desarrollo e implementación de medidas de seguridad criptográfica para proteger las comunicaciones gubernamentales.

Además, estos se encargan de proporcionar asesoramiento y certificación para los productos y servicios criptográficos para su uso en el gobierno y la certificación de estos productos y servicios para la contratación de los gobiernos y administraciones. Estos estándares representan una parte de una política de borrado seguro y es importante que se consideren todos los aspectos de esta política para garantizar la seguridad de los datos.

Cuando se habla y escribe sobre la seguridad informática, se suelen destacar aspectos críticos como la protección frente a malware, la implantación de firewalls, VPN, el uso de redes corporativas, la encriptación de los archivos o la realización de copias de seguridad periódicas. Sin embargo, hay un punto crítico que en España normalmente es olvidado y confundido a pesar de suponer una cuestión clave para proteger la confidencialidad de los datos y mantener la cadena de custodia.

Esta es la necesidad de realizar mediante procedimientos seguros un borrado de los documentos que se encuentran almacenados, como medida de saneamiento de los backups, la obligatoriedad de uso en exclusividad de los CRM corporativos, en caso de reutilización de cualquier tipo de soporte o destrucción de los mismos.

Los Centros Criptológicos de las Principales Potencias

El **Bundesamt für Sicherheit in der Informationstechnik (BSI),** es el organismo federal de seguridad de Alemania para la tecnología de la información. El BSI diseña la seguridad de la información en la digitalización a través de la prevención, detección y respuesta para el Estado federal alemán. Fue fundada en 1991 con la Ley de la Oficina Federal de la Información (BSIG), surgiendo de la Oficina Central para la Seguridad de la Información (ZSI).

El BSI es responsable de desarrollar e implementar estándares de seguridad criptográfica para la comunicación gubernamental y proteger las comunicaciones gubernamentales contra ataques cibernéticos. También proporciona asesoramiento criptográfico y capacitación a las agencias gubernamentales y a las organizaciones privadas que trabajan con el gobierno.
Además, Alemania tiene varias regulaciones y leyes que rigen la eliminación segura de datos, en sus estándares de borrado destaca el estándar VSITR de 7 pasadas de sobrescritura. En ellos se establece la necesidad de combinar 2 pasadas escritura de datos aleatorios con borrado de datos vía firmware.

De igual forma destaca la guía BSI-DSZ-CC-11-2, que proporciona una guía para la eliminación segura de datos en dispositivos móviles y de almacenamiento externo físicos y lógicos, especificando los procedimientos para garantizar la eliminación de los datos.

NCSC: el Centro Criptológico de Reino Unido

El NCSC, es el Centro Nacional de Seguridad cibernética del Reino Unido, con sede en Londres. Se constituyó tras la fusión del (CESG), Communications-Electronic Security Group, y del (GCHQ), Cuartel General de Comunicaciones del Gobierno, así como del Centro de Evaluación Cibernética, CERT-UK.

El NCSC, es responsable de desarrollar e implementar estándares de seguridad criptográfica para la comunicación gubernamental y proteger las comunicaciones gubernamentales contra ataques cibernéticos. También proporciona asesoramiento criptográfico y capacitación a las agencias gubernamentales y a las organizaciones privadas que trabajan con el gobierno.

En el Reino Unido, hay varias regulaciones y leyes que rigen la eliminación segura de datos, bajo las siglas del IS5 es parte de una familia más grande de estándares de seguridad de TI publicados, donde se establece una amplia gama de requisitos, no solo los detalles técnicos de la sobreescritura de datos, sino también las políticas y los procesos que las organizaciones deben implementar para garantizar que los medios se eliminen de forma segura.

Las guías IS5 también aborda la acreditación de la gestión de riesgos, porque la reutilización y eliminación seguras de los medios es un control importante para las organizaciones que manejan datos. No basta con desinfectar los medios; el saneamiento también debe ser auditable y se deben mantener registros.

Los estándares de borrado son creados por el NCSC, establece actualmente, el HMG (Her Majesty’s Government) e Infosec Standard 5 define 2 métodos.

Uno de ellos con una pasada de sobreescritura, cada sector del medio de almacenamiento una vez con ceros siendo el otro de 3 pasadas completas, cada sector se sobrescribe primero con 1, luego con 0 y luego con 1 y 0 generados aleatoriamente denominado CESG CPA-Higher Level, el cual requiere verificación tras cada paso.

NICT: el Centro Criptológico de Japón

El Centro Criptológico de Japón es el National Institute of Infortmation and Communications Technology (NICT), institución dependiente del gobierno japonés, tiene un sección dedicada a la criptografía y la seguridad de la información, que se encarga de establecer estándares y políticas de seguridad cibernética para el gobierno y para el sector privado de Japón.

El JAPAN JIS Q 27001 es el estándar japonés para la gestión de la seguridad de la información que proporciona un marco para establecer, implementar, mantener y mejorar la seguridad de la información en Japón.

CSE: el Centro Criptológico de Canadá

El Centro Criptológico de Canadá es el Communications Security Establishment (CSE) es el organismo responsable de la seguridad criptográfica y la inteligencia cibernética del gobierno de Canadá. La misión del CSE es proteger las comunicaciones y la información del gobierno de Canadá, así como proporcionar información al gobierno frente a las posibles amenazas que pueda sufrir el país.

Trabaja con estrecha colaboración con otras organizaciones canadienses como el (CSIS) Servicio de Seguridad del Canadá y el (CSA) Agencia de Ciberseguridad del Canadá. El CSE desarrolla estándares de seguridad, respecto al borrado ha estandarizado el Canadian RCMP TSSIT OPS-II Estándar Wipe, (Royal Canadian Mounted Police” TSSIT con “Technical Security Standard for Information Technology”), este estándar realiza siete sobre escrituras con verificación.

Los Centros Criptológicos de Estados Unidos

El Departamento de Defensa (DoD) es el órgano encargado de coordinar y supervisar todas las agencias y funciones del gobierno directamente relacionadas con la seguridad nacional y la Fuerzas Armadas, dentro y fuera de las fronteras norteamericanas.

A finales de los 90, el Departamento de Defensa de los Estados Unidos emitió la directiva AR 380-19 que establece los requisitos de seguridad para el manejo de la información en la organización. Esta directiva establece los requisitos para garantizar la seguridad de la información en la organización y se aplica a todos los empleados, contratistas y otras partes interesadas, además de los requisitos para la protección de la información crítica, la identificación y la protección de los activos de información, la protección de la infraestructura de TI y la preparación para situaciones de emergencia.

El Departamento de Defensa también especifica los requisitos para la clasificación de la información, la seguridad de los datos almacenados, la seguridad física y la aplicación de políticas de seguridad. Además de para la auditoría de la seguridad de la información y la gestión de incidentes

Se requiere que el Departamento de Defensa monitoree y revise periódicamente los requisitos y procedimientos para garantizar que la organización cumpla con esta directiva en los servicios nacionales de Inteligencia.

- La Agencia de Inteligencia de Defensa (DIA). Su función es la de análisis de las estrategias de combate y del aseguramiento de las defensas, así como la evaluación de los datos de inteligencia y las características, el rendimiento, las operaciones y las vulnerabilidades de los sistemas de ciberarmas mundiales.z

- La Agencia de Seguridad Nacional (NSA). La NSA es responsable de la seguridad criptográfica de las comunicaciones gubernamentales y militares, así como de la recopilación de inteligencia cibernética y la prevención de ataques cibernéticos enemigos.
- La Agencia Nacional de Inteligencia-Geoespacial (NGA). La NGA es una combinación única de agencia de inteligencia y agencia de apoyo de combate, cubre desde los fondos marinos al espacio exterior en las comunicaciones y custodia de información electrónica.
- La Oficina Nacional de Reconocimiento (NRO). La NRO diseña, construye, lanza y opera satélites de reconocimiento, mediante la obtención y entrega de inteligencia satelital.
- La Agencia de Ciberseguridad y Infraestructura (CISA). CISA es responsable de proteger las infraestructuras críticas de Estados Unidos contra ataques cibernéticos.
- La Agencia de Defense de los sistemas de Información (DISA). La DISA es responsable de proporcionar servicios de seguridad cibernética y criptográfica al Departamento de Defensa de Estados Unidos.
- El Departamento de Estado (DoS). El Departamento de Estado de los Estados Unidos, es el departamento federal responsable de las relaciones internacionales y de la política exterior de Estados Unidos. En su estructura se encuentra la Agencia de Seguridad y las comunicaciones, Diplomática, encargada de la seguridad de las embajadas y de los órganos diplomáticos norteamericanos.
- El Departamento de Justicia (DoJ). El Departamento de Justicia administra diversas agencias federales encargadas de velar por el cumplimiento de la ley como la Oficina Federal de Investigación (FBI), el Servicio de Marshals de Estados Unidos (USMS), la Agencia de Alcohol, Tabaco, Armas de Fuego y Explosivos (ATF), la Agencia control de Drogas (DEA) y la Agencia Federal de Prisiones (Bop).
- National Institute of Standards and Technology (NIST). NIST es la entidad responsable de desarrollar y promover estándares y guías de seguridad cibernética para el gobierno y el sector privado. Fundado en 1901, es la agencia del Departamento de Comercio, encargada de las acreditaciones y guías de la tecnología de medición, para agencias federales y proveedores de infraestructuras críticas.

En 2006 el NIST, publico la guía NIST 800-88, para la eliminación segura de datos en medios físicos y lógicos, especificando los procedimientos para garantizar la eliminación de los datos, que contempla dos procedimientos diferentes para alcanzar el objetivo de borrado (impide recuperación de los datos mediante software) y purgado (impide recuperación de los datos en laboratorio).

NSO: Oficina de Normalización de la OTAN

La Oficina de Normalización de la OTAN (NSO), coordina, apoya, administra y asiste al Comité Militar de la OTAN en el desarrollo de estándares operativos militares, que se llevan a cabo bajo la autoridad del Comité de Normalización (CS), el comité responsable de la política de normalización.

La OTAN también ha desarrollado una serie de iniciativas y estrategias para mejorar la Seguridad Nacional, incluida la Estrategia de Seguridad de la OTAN (NSD), que define los principios básicos de la seguridad de la OTAN.Esta estrategia se centra en la prevención de conflictos, la cooperación regional y la construcción de la paz. De acuerdo con la Estrategia C3 de la Alianza se recomienda a todos los países aliados adherirse a dichos estándares y perfiles para asegurar la interoperabilidad en el marco de la OTAN y entre países. Estos estándares y perfiles son obligatorios para los aliados que se integren en una red federada implantada para una misión dirigida por la OTAN. A través del Programa Nacional de Seguridad Industrial (NISP) programa diseñado para proteger la seguridad de la información clasificada en las organizaciones industriales de Estados Unidos, dirigido a todos los actores de los países de la alianza que participan en el desarrollo, implantación, gestión del ciclo de vida y transformación de los CIS/TIC.

Además, establece los estándares correspondientes a diferentes organismos de normalización reconocidos internacionalmente. Los estándares y perfiles obligatorios incluidos en el NISP se aplican en los sistemas comunes financiados por la OTAN.

Además, las naciones participantes se comprometen a utilizar dichos estándares y perfiles obligatorios en los Puntos de Interoperabilidad de Servicios y utilizar los perfiles de interfaz de servicio entre la OTAN y las naciones para el intercambio de información y el uso de los servicios de información en el ámbito de la OTAN.
El NATO STANAG 4406 es el estándar de la OTAN que proporciona directrices para la seguridad de la información en las organizaciones militares de la OTAN, que consiste en siete pasadas de sobrescritura. En las primeras seis pasadas se utilizan los valores fijos alternativos entre cada pasada: (0×00) y (0xff). En la séptima pasada se emplea un carácter aleatorio.

La normal internacional de los Centros Criptológicos

La norma internacional de seguridad de la información ISO 27001 establece las mejores prácticas para la gestión de la seguridad de la información, incluyendo la eliminación segura de datos. Los Estándares de la Industria de ADISA se aplican a las empresas que participan en la recuperación y eliminación de activos de TI, el arrendamiento, la logística y las reparaciones.

El proceso de borrado seguro, de documentación electrónica y soportes informáticos, debe estar integrado en la política de gestión de documentos electrónicos y la política de seguridad corporativa, en el denominado Sistema de Gestión del Borrado Seguro de Datos (SGBSD) de la organización.Además, debe acomodarse al Anexo II del Esquema Nacional de Seguridad en su punto 5.5.5, donde se establecen las condiciones necesarias de confianza para ello que incluyen las medidas y procedimientos que se han dispuesto legalmente para la eliminación de documentos que no requieren conservación permanente. En el caso español, el uso del software de algoritmos de cifrado para el borrado debe estar acreditado y certificado por el Centro Criptológico Español recogido en sus guías es de uso obligatorio para el borrado seguro y certificado, previo todo ello a la destrucción física si fuera el caso, nunca como alternativa.

A nivel mundial se han reconocido varios estándares de borrado de datos. Los criterios que distinguen a cada uno de ellos están principalmente relacionados con el número de pasadas de sobrescritura, así como las características de los algoritmos empleados (fijos o aleatorios):

- **Algoritmo de borrado lineal:** este algoritmo se basa en recorrer todos los elementos de una lista uno por uno y eliminar aquellos que cumplan con una condición predefinida.
- **Algoritmo de borrado binario:** este algoritmo se basa en la utilización de una búsqueda binaria para encontrar el elemento que se desea eliminar. Una vez encontrado, se elimina el elemento y se reajustan los enlaces de la lista.
- **Algoritmo de borrado por valor:** este algoritmo se basa en recorrer toda la lista y eliminar aquellos elementos que tienen un valor determinado.
- **Algoritmo de borrado por índice:** este algoritmo se basa en encontrar el elemento utilizando un índice y luego eliminarlo de la lista.
- **Algoritmo de borrado por dirección:** este algoritmo se basa en encontrar el elemento utilizando su dirección en memoria y luego eliminarlo de la lista.

El empleo de un estándar específico dependerá de los protocolos o requisitos internos de seguridad propios de cada empresa u organismo público.

Para más información sobre soluciones para borrado seguro y certirficado, visite **www.deletetechnology.com**

Autor,z
Rafael Chust Calero
Director Delete Technology España & Portugal

Av. Ejército Nacional 826A Oficina 104 Col. Polanco CDXM 11540 México

Delete Technology

Powered by blancco