Delete Technology

www.deletetechnology.com

5 Mejores prácticas para la destrucción de datos con NIST.

La reciente actualización del **Instituto Nacional de Estándares y Tecnología (NIST)** del documento **800-88** directrices para el borrado de medios se centra en los medios de acuerdo con el nivel de datos confidenciales almacenados en los medios de almacenamiento. Después de que una organización tiene una claridad de los riesgos de una posible violación o fuga de datos, es posible determinar las herramientas de destrucción de datos, los métodos de registro y la estrategia general para el retiro de los medios de almacenamiento. Este documento divide **5 consejos para implementar un programa seguro de desinfección y disposición de medios.**

No. 1 Clasificar los medios de almacenamiento de datos según el nivel de confidencialidad de los datos y riesgo asociado .

Clasificar los medios de una organización por nivel de confidencialidad de datos tiene sentido tanto para la eficiencia operativa de un departamento de **TI** como para la estrategia general de seguridad de datos. **NIST** aconseja a las organizaciones que determinen el nivel de confidencialidad de acuerdo con el riesgo de una posible fuga de datos. Aparte de las multas y tarifas asociadas con la filtración de información confidencial de empleados y clientes, una organización debe sopesar los riesgos de pérdida de ingresos por pérdida de negocios futuros o gastos por la divulgación no deseada de la propiedad intelectual y la estrategia de la empresa. Una vez que una organización tiene una comprensión de los riesgos asociados a cada medio de almacenamiento de datos, puede determinar los métodos y la atención adecuada y necesaria para implementar un proceso de destrucción de datos. Por ejemplo, una organización puede sentir que discos duros específicos de un departamento de diseño gráfico no son un riesgo de exposición, sino que todos los discos duros del departamento de contabilidad deben clasificarse como confidenciales.

Delete Technology blancco

En este escenario, el área de seguridad de la información o gerente de **TI** puede optar por poner en juego políticas menos estrictas para los discos duros del departamento de diseño gráfico, al tiempo que coloca una política de destrucción de datos, verificable, registrada y certificada para los datos del departamento de contabilidad. En lo que respecta al retiro, la dirección de **TI** debe asegurarse que, al salir de la custodia de la empresa, los discos duros deben ser borrados de manera segura **(purga según el NIST)** de acuerdo con los diversos niveles de confidencialidad asignados.

No.2 Elegir directivas de destrucción de datos según la fase del ciclo de vida y el destino de los medios

Una vez que su organización comprende la jerarquía de riesgos y ha categorizado los medios en consecuencia, la directiva de destrucción de datos puede ser impulsada por el lugar donde los medios se encuentran en la **etapa del ciclo de vida.** Los medios que se transfieren o vuelven a utilizar en una organización pueden tener un estándar de destrucción de datos diferente que los discos duros que se retirarán y eliminarán. Su organización puede optar por destruir físicamente los discos duros que tienen daño físico y por lo tanto no pueden ser borrados de manera segura. Los discos duros altamente confidenciales deben pasar por el borrado de borrado seguro, mediante una sobreescritura de datos con verificación para su reutilización interna.

La verificación y documentación de los métodos de destrucción de datos también debe elegirse de acuerdo con el ciclo de vida. La selección del tipo de método de sobreescritura de destrucción también estará impulsada por la etapa del ciclo de vida del medio. Es posible que no sea posible reutilizar ciertos tipos de medios que han sido desgausados o alterados físicamente. En algunos casos, una organización puede optar por borrar los discos duros con el estándar de borrado NIST I de 1x sobreescritura a los discos duros antes de ser reutilizados o utilizar un estándar de borrado **HMG INFOSEC** para discos duros confidenciales.

Para cada proceso de borrado debe de documentar la destrucción de datos durante la reutilización interna y las transferencias de equipos de cómputo, pero antes de la disposición una organización debe requerir documentación y certificación de firma independientemente del nivel de confidencialidad de los datos.

No.3 Aprobar y utilizar las herramientas de destrucción de datos adecuadas

Las organizaciones deben de seleccionar un software para realizar varios niveles de destrucción de datos. Estas herramientas se pueden administrar internamente o una organización puede depender de proveedores para ciertas funciones, pero de cualquier manera el proceso debe incluir pasos para verificar el éxito de las herramientas.

Es necesario contar con una herramienta que ofrezca diferentes soluciones para el borrado seguro de datos. Por ejemplo, si la limpieza o purga de datos es el método preferido de una empresa para todos los medios, los productos disponibles para hacerlo pueden no ser compatibles con ciertos sistemas y plataformas. Las fallas mecánicas y los sectores defectuosos (remapeados) también pueden hacer imposible un borrado seguro. En estos casos, una empresa debe mantener un procedimiento de borrado seguro para **discos duros (HDD)** y otro para **discos de estado sólido (SSD)**, Tal vez el ejemplo más prudente a destacar son los métodos aprobados para la erradicación de datos de **disco de estado sólido (SSD)**. El documento actual de ***NIST aprueba clear, purge, and destroy para SSD***. Debe tenerse en cuenta específicamente que degausear un disco de estado sólido SSD no destruye los datos en los discos, ya que los **SSD** no utilizan tecnología magnética para almacenar información. **NIST** continúa destacando que él borrado seguro y la limpieza de **SSD** requiere verificación, comprobaciones manuales por parte de los técnicos de que los datos se han borrado y, por lo general, verificaciones de calidad de la administración en la implementación del proceso general.

No.4 Reporte de Borrado será la evidencia del proceso

Una característica clave para cualquier destrucción de datos y política de seguridad al final de la vida útil es desarrollar un reporte de borrado y un lugar para depositar los reportes para atender las auditorias internas o externas. El reporte deberá contar con cierta información que va enfocado en capturar detalles clave a lo largo de los procedimientos de destrucción. **NIST** hace hincapié en los elementos clave a tener en cuenta de la siguiente manera:

- **Nivel de Confidencialidad (Estándar de Sobreescritura)**
- **Herramienta Utilizada (incluir versión, marca, marca y/o modelo)**
- **Método de Verificación (Comprobación manual completa, muestra rápida, etc.)**
- **Reporte auditable y que no sufra alteraciones posteriores a su generación**
- **Nombre de la persona responsable, título, fecha, ubicación e información de contacto**
- **Firma de la persona**

No.5 Reporte de Borrado será la evidencia del proceso

Un procedimiento de destrucción de datos seguro debe incluir la verificación de la eliminación de datos a través de herramientas de generación de reportes integradas en los productos de borrado seguro disponibles, así como certificaciones completas para verificar y garantizar el éxito de la eliminación de datos.

La dirección de **TI** también debe requerir que la gerencia de seguridad supervise y realice evaluaciones de desempeño para evaluar que el trabajo que se está realizando.

Los procesos de borrado seguro de datos no solo deben de orientarse con niveles de seguridad, sino que la herramienta de borrado y los reportes del proceso garanticen que la empresa está en cumplimiento a normativas y regulaciones en protección de datos.

2020-08-18 21:02:45 (+0000), BLANCCO DRIVE ERASER 6.8.0, DELL INC., LATITUDE 7480, 1XM55H2

Data Erasure Report

blancco

Licensed To Banco

Custom Fields

Nombre Del Cliente:	Banco	Edificio:	REFORMA
Número De Serie Del Equipo Borrado:	D5YZNH2	Hostname Del Equipo Borrado:	MB80867
Personal Que Realiza El Borrado:	usuario final	Usuario De Red (XM-MB):	XM10088
Comentarios:	N/A		

Erasure Results

Disk:	Vendor: **Micron** Size: **256GB** HPA: **Doesn't exist** Health Status: **good**	Model: **1100 SATA 256GB** Bus: **SATA/SSD** DCO: **Doesn't exist**	Serial: **17361930F3E6** Sectors: **500118192** Remapped Sector(s): **104**
Remapped Sector(s) After Erasure:	**104**		
Start/End Time:	**2020-08-18 13:48:03 (-0500) / 2020-08-18 15:20:29 (-0500)**		
Duration:	**01:32:26**		
Method:	**Blancco SSD Erasure - ATA**		
Erasure Rounds:	**4 (2 overwriting, 2 firmware based erasure)**		
Status:	**Erased**		
Information:	**Device is SSD, see manual for more information. Remapped sectors area erased.**		

Hardware Details

Manufacturer:	Dell Inc.
Chassis Type:	Notebook
Model:	Latitude 7480
Serial:	1XM55H2
UUID:	4C4C4544-0058-4D10-8035-B1C04F354832
Processor:	GenuineIntel, Intel(R) Core(TM) i7-7600U CPU @ 2.80GHz, Cores: 2, Stepping: 9, Nominal speed: 2300MHz, Max speed: 3900MHz, External Clock: 100 MHz
Memory Bank:	80AD000080AD, 8192MB, 2400MHz, Synchronous Unbuffered (Unregistered), SODIMM, Serial: 420D8515
Memory Bank:	Unknown Vendor, Empty slot, DIMM
Total Memory:	8192MB, Occupied memory banks: 1/2
Graphics Card:	Intel Corporation HD Graphics 620, 256MB
Current Resolution:	1366x768
Sound Card:	Intel Corporation Sunrise Point-LP HD Audio
Storage Controller:	Intel Corporation Sunrise Point-LP SATA Controller [AHCI mode]
Disk:	Micron, 1100 SATA 256GB, Firmware: M0DL003, Serial: 17361930F3E6, 256GB / 500118192 sector(s), SATA/SSD, Sector Size: 512, Average Write Speed: 91MB/s, Average Read Speed: 301MB/s, Accessible Region: 256GB / 500118192 sector(s), DCO: Doesn't exist, HPA: Doesn't exist, Remapped Sector(s): 104, Health Status: good
Network Adapter:	Wireless, Intel Corporation Wireless 8265 / 8275, f8:59:71:62:06:06
Network Adapter:	Ethernet, Intel Corporation Ethernet Connection (4) I219-LM, d4:81:d7:c0:14:aa, 150.216.15.250, 255.255.255.0, 150.216.15.1
USB Device:	Intel Corp., Unknown 2.00
USB Device:	Sunplus Innovation Technology Inc., Unknown, CNFGH19N172031008F92, Integrated_Webcam_HD 2.00
USB Device:	Broadcom Corp., Unknown, Broadcom Corp, 5880 1.10
USB Device:	Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.), Flash Drive, SMI Corporation, USB DISK 2.00
Motherboard:	Dell Inc., 0CXWHP
BIOS:	Dell Inc., Version: 1.14.1, Date: 04/03/2019
BIOS Features:	PCI, PNP, ACPI, CD Boot, EDD, Legacy USB
Ports:	USB Ports: 3, HDMI: 1
Battery:	Vendor: SMP, Model: DELL DM3WC64, Serial: 3223, Type: Li-poly, Capacity: 100 / 7895 mAh, Voltage:8079 mV

Report Details

Report UUID:	fbeb995f-80f0-4893-8e0f-c462e7b90bd5
Report Date:	2020-08-18 21:02:45 (+0000)
Software Version:	Blancco Drive Eraser 6.8.0

Digital Signature:

lo5YzdsXyQfrJuOtHScLKkc4EhEDDHFMYtyickXfvTpv2CFuiT2QHUqV/BrjEZskqXxdKpX9tPA/2Nl4RrZUX/rlvmnIw+4E/1tIQNsdWgXsrW4Hb+SD/txmMGmHPhLQqukLGt1MS6xaRuDvN1sh/2gTZpVTkwA7iKUIUUu+th3GNh
eAXAV0GOfSNJxaByy5ISqNEJsWsNOi7U9SHNMuKAbGJb/0qFQjG3bytF1y56x5hMuc4/VpYhELWmvLmAyFUvebgpBZ4G4TgrZsC+QVjg3jdrHq33b4Sb12IoAiPnMkprzoNkZgyOjka4Fta+lE8YkgaTiZ0r1pC8N+pvFy7g==

Delete Technology

Delete Technology S.A de C.V
Av.Ejército Nacional 826-A Oficina 104
Polanco, Miguel Hidalgo 11540 CDMX.
Tel: 55 4627-4100