



**BORRADO SEGURO Y CERTIFICADO
DE INFORMACIÓN**



INTRODUCCIÓN

No hay nada más perturbador para alguien responsable del gobierno de los datos que saber lo que no saben cuando se trata del estado de sus datos. ¿Dónde se almacenan los datos críticos? ¿Qué datos reside en cada dispositivo? ¿Los discos duros y los sistemas que se van a reciclar están limpios de todos los datos corporativos?

Llegar a la etapa de saber lo que no sabe es el primer paso del viaje hacia una política integral de eliminación de datos. Este documento describe cómo completar el viaje a través de la gestión integral del ciclo de vida de los activos y la gestión del ciclo de vida de datos.

ALGUNAS CONSIDERACIONES

El objetivo final de una política de administración del ciclo de vida de los datos y los activos es reducir el riesgo de incumplimiento y pérdida de datos para la organización. Hacerlo a un costo mínimo e incluso recuperar el valor de los discos duros y dispositivos es un beneficio de esta política que justifica la inversión inicial.

Requisitos de retención de datos: La mayoría de los países y sectores industriales tienen regulaciones específicas que dictan tiempos mínimos de retención de datos. Los servicios financieros a menudo se requieren para mantener todos los registros hasta por siete años. Algunas agencias gubernamentales requieren que los datos se archiven para siempre.

Durante el proceso de descubrimiento en una acción legal civil o regulatoria, se deben preservar todas las clases de datos. Esto significa que los sistemas deben estar en su lugar para detener la implementación de los procedimientos de borrado de datos.

Derrame de datos: Los datos confidenciales se pueden copiar inadvertidamente a un sistema o aplicación no autorizados. Los datos no solo deben borrarse, sino que deben borrarse completamente.

Manejo de archivos clasificados como confidenciales.

Un empleado, consultor o tercero puede recibir datos confidenciales que almacenan en su sistema. Después de que los datos o el documento hayan cumplido su propósito, deben borrarse de forma segura del sistema para evitar posibles fugas de datos. Una rutina automática para borrar de forma segura la papelera de reciclaje regularmente es una implementación fácil. También se pueden implementar políticas granulares para borrar de forma segura tipos de archivos específicos por número de revisión y sello de tiempo.

Migración de Datos:

Cada vez que los datos se mueven de una ubicación a otra, de un servidor retirado a un nuevo servidor, de una máquina virtual a otra, la ubicación de los datos originales debe borrarse. El borrado es necesario para la reutilización de LUN en un entorno alojado cuando un usuario migra a un LUN más grande o abandona la nube, para que el LUN pueda ser reasignado de manera segura a un nuevo usuario. Esto es cierto tanto para los servidores físicos que usan LUN como almacenamiento y para las máquinas virtuales con almacenamiento dedicado en un LUN particular. Esto cumple con la norma ISO27018.

Fin de la vida útil para máquinas virtuales clasificadas:

La nube implica un cambio constante de las máquinas virtuales a medida que se giran, se duplican y se eliminan. Cada vez que se desactiva una VM, se debe borrar por completo, junto con las instantáneas de memoria que se hayan tomado. Debería poder lograr esto sin reiniciar el host. Al instalar la solución de borrado en el nivel de VMware ESXi, puede borrar manualmente las máquinas virtuales en VMware vSphere. Todos los archivos asociados con las máquinas virtuales objetivo deben ser borrados, incluyendo VMDK, VMSD, VMX y VMXF. Todas estas características demuestran por qué la UEBA se está convirtiendo en una parte tan importante de la seguridad de la red. Y la UEBA efectiva a través del conocimiento amplio del usuario es la mejor forma de detectar comportamientos maliciosos. Con el fin de proporcionar una gestión de identidad significativa y lograr una alta garantía de eventos anómalos, las empresas deben confiar en el análisis del comportamiento de la entidad, el usuario de la red y el punto final. Solo así podrán obtener el mejor valor de sus inversiones en la UEBA.

En la demanda de los clientes:

Muchos NDA estipulan que al final del término de un contrato, todos los datos compartidos deben ser eliminados. Se debe proporcionar un certificado de eliminación para demostrar que los términos del contrato tienen cumplido.

Además, en jurisdicciones como la UE, el “derecho a ser olvidadas” las reglas dictan que si los consumidores te preguntan para eliminar sus datos de sus servidores, debe cumplir. No es suficiente simplemente borrar el registro. En su lugar, debe ser completamente eliminado sin cualquier posibilidad de volver para perseguirlos. Un ebe existir un registro de auditoría con un informe certificado para demostrar que se produjo el borrado. Incluir copia de seguridad y procedimientos de recuperación para evitar el potencial de tener los datos borrados vuelven a aparecer en la base de datos de producción.

LISTA DE VERIFICACIÓN:

- ✓ *Descubre donde residen tus datos*
- ✓ *Determine el final de la vida útil para cada tipo de datos.*
- ✓ *Construir una política para la destrucción de datos.*
- ✓ *Crear un horario consistente para la destrucción de datos.*
- ✓ *Cree un proceso para la desinfección de dispositivos, incluidos equipos de escritorio, portátiles, dispositivos móviles, servidores y unidades de disco duro perdidas.*

donde los datos reales del cliente se utilizan normalmente en la prueba. Debido a esto, es fundamental borrar los datos del sitio secundario. En cualquier caso, una vez que se restauran los sistemas de producción, todos los datos que queden en los discos de recuperación deben borrarse. Esto también podría aplicarse a "ejercicios de prueba" o escenarios similares cuando se usan datos reales

Siete pasos para crear un proceso de sanitización de datos

El Instituto Nacional de Estándares y Pruebas (NIST) describe siete (7) pasos para crear un marco de ciberseguridad global. Estos pasos también son aplicables para crear un proceso completo de desinfección de datos.

Paso 1. Priorizar y Alcance. La Compañía reconoce los riesgos asociados con la falta de control sobre la información a lo largo de su ciclo de vida y además reconoce la necesidad de un enfoque del ciclo de vida de la información que implique procesos adecuados de desinfección de datos en cada paso. Se identifican aplicaciones y almacenes de información particulares que se encuentran dentro del alcance de esta política. Los recursos se dedican al saneamiento de datos a medida que se implementa esta política. El alcance del programa se decide a partir de la información de mayor prioridad. Los tipos de información que podrían estar dentro del alcance incluyen, pero no se limitan.

- Registros de empleados (salud, desempeño, acciones disciplinarias, financieros)
- Registros de clientes
- Información de identificación personal
- Correo electrónico y otras comunicaciones corporativas.
- Documentos legales (contratos, memorandos de entendimiento, presentaciones públicas)
- Registros de transacciones
- Propiedad intelectual (patentes, notas, registros de investigación)
- Material de marketing
- Documentación de atención al cliente
- Documentación de calidad de fabricación.
- Registros que no han sido anónimos

Paso 2. Orientar. Una vez que se ha determinado el alcance del programa de desinfección de datos para la línea de negocios o el proceso, la organización identifica los sistemas y activos relacionados, los requisitos reglamentarios y los riesgos generales de exposición de datos. Esta auditoría de datos abarcará todos los tipos de datos recopilados almacenados, procesados, archivados y eliminados. La organización luego identifica las amenazas y vulnerabilidades de los almacenes de datos, sistemas y activos utilizados para procesar esos datos.

Paso 3. Crea un perfil actual. Mapear el estado de los procesos existentes con la documentación de respaldo. Determine, cuando sea necesario, el método adecuado de desinfección de datos.

Por ejemplo, haga un mapa del proceso por el cual se incorporan los nuevos clientes y cómo se crean y mantienen los registros a medida que sus pedidos se cumplen, se entregan, se facturan y se contabilizan los pagos. A medida que los registros envejecen, ¿cómo se archivan? ¿Por cuánto tiempo? ¿Existe una política de retención de registros para cada entorno regulatorio? ¿Cuál es el procedimiento apropiado para deshacerse de esos registros al final de su vida?

Paso 4: Realizar una evaluación de riesgos. Identifique el riesgo de una acción regulatoria, incluidas multas y supervisión, impuesta por los reguladores con base en el Perfil actual. Luego, cuantifique el riesgo para la organización derivado de la eliminación incorrecta de los datos, incluida la pérdida de la propiedad intelectual, los costos de notificación de infracciones y el impacto en la marca y la satisfacción del cliente.

Paso 5: Crear un perfil de destino. Se establecen metas para la gestión de saneamiento de datos. El Perfil objetivo es el estado final deseado: un programa de desinfección de datos completamente implementado dentro del alcance definido en el Paso 1. Para cada clase de información priorizada, se define su fin de vida útil (período de retención) y se aplica la desinfección de datos adecuada. Para la mayoría de la información que conlleva la sobrescritura de software certificada, pero es posible que algunos equipos deban ser destruidos físicamente y que se mantengan registros de esa destrucción.

Paso 6: Determine, analice y priorice las brechas. Determine qué tecnología, procesos y personas deben pasar del Perfil actual al Estado objetivo. Por ejemplo, se puede determinar que no existe un proceso establecido para la limpieza permanente de archivos temporales, como los generados por la actividad de navegación. Se implementa un plan para implementar el software cliente que puede desinfectar automáticamente los archivos temporales. Otro ejemplo de una brecha puede ser la forma en que el hardware en un centro de datos se devuelve al fabricante para su garantía. Será necesario implementar un proceso completo de desinfección del disco para cerrar esta brecha.

Paso 7. Implementar el Plan de Acción. Trabajar sistemáticamente para cerrar brechas y mejorar continuamente las prácticas de desinfección de datos. Cree hitos medibles y vuelva a visitar la etapa de alcance al menos una vez al año.

Desinfección de datos definida

La desinfección de datos es el proceso de eliminar o destruir, de forma deliberada, permanente e irreversible, los datos almacenados en un dispositivo de memoria para hacerlos irrecuperables. Un dispositivo que ha sido desinfectado no tiene datos residuales utilizables, e incluso con la ayuda de herramientas forenses avanzadas, los datos no se pueden recuperar. Existen tres métodos para lograr la desinfección de datos: destrucción física, borrado criptográfico y borrado de datos.

Dstrucción Física

El proceso de trituración de discos duros, teléfonos inteligentes, impresoras, computadoras portátiles y otros medios de almacenamiento en pequeñas piezas mediante trituradoras mecánicas grandes o utilizando Degaussers.

Degaussing

Una forma de Dstrucción Física, en la que los datos se exponen al potente campo magnético de un Degausser y se neutralizan, lo que hace que los datos no se puedan recuperar. La desmagnetización solo se puede lograr en las unidades de disco duro (HDD) y en la mayoría de las cintas, pero las unidades o cintas no se pueden reutilizar una vez finalizadas. La desmagnetización no es un método efectivo de desinfección de datos en unidades de estado sólido (SSD).

Pros & Contras de la Dstrucción Física

La destrucción física es un método eficaz de destruir datos para hacerlos irrecuperables y lograr el saneamiento de los datos. La destrucción física puede ser perjudicial para el medio ambiente y destruye los activos por lo que no se pueden reutilizar ni revender. A menudo requiere el transporte de medios a una instalación de procesamiento, lo que conlleva riesgos asociados con el control de los dispositivos.

Borrado Criptográfico (Crypto Erase)

Borrado criptográfico es el proceso de usar software de cifrado (ya sea integrado o implementado) en todo el dispositivo de almacenamiento de datos, y borrar la clave utilizada para descifrar los datos. La mayoría de las organizaciones utilizan una longitud de clave de cifrado de 256 bits. Mientras que los datos permanecen en el dispositivo de almacenamiento, al borrar la clave original, los datos son imposibles de descifrar. Como resultado, los datos se vuelven irrecuperables y es un método apropiado para lograr el saneamiento de los datos. Dicho esto, la mayoría de las organizaciones no tienen una política de administración de claves completa y, a menudo, almacenan las claves en lugares accesibles como Active Directory.

Pros y Contras de la Eliminación Criptográfica

El borrado criptográfico es un método eficaz y rápido para lograr la desinfección de datos y se utiliza mejor cuando los dispositivos de almacenamiento están en tránsito o para dispositivos de almacenamiento que contienen información que no es confidencial. El borrado criptográfico se basa en gran medida en el fabricante donde podrían producirse problemas de implementación. Los usuarios también podrían afectar el éxito de la eliminación criptográfica a través de claves rotas y errores humanos. Pero lo más importante es que el borrado criptográfico todavía permite que los datos permanezcan en el dispositivo de almacenamiento y, a menudo, no cumplen con los requisitos de cumplimiento normativo.

Borrado de Datos

El método basado en software para sobrescribir de forma segura los datos de cualquier dispositivo de almacenamiento de datos utilizando ceros y unos escritos en todos los sectores del dispositivo. Al sobrescribir los datos en el dispositivo de almacenamiento, los datos se vuelven irre recuperables y logran la desinfección de los datos.

Requisitos para el software Data Erasure:

- 1.El software Data Erasure permite la selección de un estándar específico, basado en las necesidades únicas de su industria y organización.
2. El software Data Erasure verifica que la metodología de sobrescritura ha sido exitosa y ha eliminado los datos de todo el dispositivo, o los Datos de destino (si se los llama específicamente).
- 3.El software Data Erasure produce un certificado a prueba de manipulaciones que contiene información de que el borrado se realizó correctamente y se escribió en todos los sectores del dispositivo, junto con los datos sobre el dispositivo y el estándar utilizado.

Pros y contras de la eliminación de datos

El borrado de datos es la forma más alta de asegurar los datos dentro de una política de desinfección de datos debido al proceso de validación que garantiza que los datos se sobrescribieron con éxito y el informe auditable. Data Erasure también es compatible con iniciativas medioambientales, al tiempo que permite a las organizaciones conservar el valor de reventa de los dispositivos de almacenamiento. Sin embargo, la eliminación de datos es un proceso más oportuno que otras formas de desinfección de datos. El borrado de datos obliga a la organización a desarrollar políticas y procesos para todos los dispositivos de almacenamiento de datos dentro de una organización.

PROCEDIMIENTOS DEL CICLO DE VIDA ACTIVA

Los procedimientos de ciclo de vida de los activos se desarrollan para garantizar que los datos digitales estén adecuadamente protegidos de la divulgación no autorizada cuando el equipo técnico o los medios de datos se están redistribuyendo dentro de la organización, se eliminan (final de la vida útil), o de cualquier otra manera, se están dejando los de la organización, o Terceros socios, control físico. Este último puede incluir servicio externo, por ejemplo, o Autorización de devolución de material (RMA) del fabricante. Este tipo de equipo contiene datos, a veces de propiedad, clasificados, confidenciales de la empresa, personales o de otro tipo, así como software que conlleva restricciones de licencia. Antes de que se produzca un cambio de control, todos los equipos técnicos capaces de almacenar o el procesamiento de datos de la empresa debe utilizar el borrado de datos Esto se puede completar dentro del departamento de TI de la compañía o un socio seleccionado también puede facilitar el borrado de datos durante el cambio de control. Estos socios seleccionados incluyen compañías de leasing que poseen.

el equipo, los socios de subcontratación que poseen y / o administran el equipo, o un profesional ITAD (IT Asset Disposal Company) contratado para sus servicios.

Con estas medidas de seguridad implementadas, el objetivo de la política es mejorar los procedimientos de la empresa para alentar la reutilización de equipos dentro de la organización o por nuevos usuarios fuera de la organización. La política de la compañía es minimizar el impacto en el medio ambiente de los equipos, prolongando su vida útil a través de la reutilización, la donación o el uso de piezas.

PROCESO SUGERIDO EN CORTO

Todos los equipos técnicos capaces de almacenar o procesar datos de la empresa deben utilizar el borrado de datos por parte de un proveedor de software de borrado de datos certificado y aprobado antes de que se produzca un cambio de control. El proceso debe permitir la documentación y la trazabilidad completas, por lo que, por ejemplo, se puede probar que un disco duro individual se borra correctamente si se lo cuestiona.

El requisito para el borrado de datos de equipos que no son propiedad de la compañía debe estar cubierto por un contrato legal con el proveedor del equipo. El equipo o los medios de datos que no se pueden borrar de forma segura pueden requerir la destrucción física.

PROCEDIMIENTOS DE BORRADO DE DATOS

Responsabilidad

El propietario del proceso es responsable de validar que el resultado de los procedimientos de borrado de datos cumpla con los requisitos establecidos en este documento. La validación de los procedimientos de borrado de datos debe realizarse anualmente, como mínimo, o cada vez que se introduzca un nuevo tipo de equipo técnico o de datos. El proceso de validación (ver abajo) debe ser documentado.

Si se contrata a un proveedor de servicios para realizar el procedimiento de borrado de datos, debe requerirse una trazabilidad completa y la validación de este trabajo debe ser realizada por LA COMPAÑÍA anualmente, como mínimo.

Como propietario del proceso, las regulaciones o la legislación externa pueden requerir que se desarrollen procedimientos específicos dentro de un proceso de negocios. Ejemplos de esto podrían ser los requisitos de PCI DSS (custodia de la información de la tarjeta de crédito) y la legislación de protección de datos (prevención de la transferencia no autorizada o el procesamiento de datos personales).

Validación de Software y equipos de borrado de datos

Todos los procedimientos de eliminación de datos deben validarse para cumplir con los requisitos establecidos en este documento. La validación debe basarse en certificaciones externas y aprobaciones de software.

Las autoridades externas de certificación y aprobación deben ser organizaciones tales como las autoridades gubernamentales de certificación, las organizaciones de defensa nacional y las autorizadas para realizar pruebas y otorgar aprobaciones para Common Criteria. Las pruebas internas basadas en un análisis exhaustivo de los medios borrados también se aprueban, si están bien documentadas y se realizan para cumplir con los estándares de la industria. Los dispositivos de almacenamiento o los medios de datos dañados deben someterse a una evaluación de riesgos para determinar si deben destruirse, repararse o desecharse. El borrado de datos utilizado en equipos técnicos o medios de datos debe registrarse para futuras consultas, manteniendo un registro de auditoría. En el caso de equipos técnicos arrendados, el contrato legal debe cubrir estos requisitos de Borrado de Datos.

Factores a Tener en Cuenta:

- ¿Existe un procedimiento de eliminación de datos validado para el tipo específico de equipo o medio involucrado?
- ¿El equipo o el soporte de datos están defectuosos y el borrado de datos está prohibido?
- En general, en el momento en que los datos cambian de ubicación, hay un cambio en el control del propietario del dispositivo, o si el dispositivo abandona la premisa de la empresa, habrá una necesidad de borrar los datos.

CONCLUSIÓN

Alguien responsable de la gestión de datos dormirá mejor por la noche, sabiendo que ha reducido significativamente el riesgo de incidentes futuros que llevan a multas, simulacros de incendio y pérdidas financieras. Han viajado desde saber lo que no saben hasta saber dónde residen sus datos y lo que les sucede al final de su vida útil.

Comience su viaje hoy mismo para implementar una política completa de eliminación de datos.

Marcos Flores

Director General Delete Technology S.A de C.V

Participó en la industria del borrado de datos desde 2006. Como consultor ha ayudado a desarrollar procesos para que los centros de datos, el gobierno, los bancos y las empresas creen políticas de borrado de datos para lograr el cumplimiento de la ley de protección de datos.

"El próximo desafío para las empresas es proteger la información en la nube a medida que dependan cada vez más de esta tecnología".

Richard Stiennon

Director de IDSC

Analista de la industria de seguridad de TI y autor que aborda temas de defensa cibernética y actores de amenazas. Stiennon es analista de la industria y asesor de muchas empresas de seguridad, desde nuevas empresas hasta las más grandes. Ha estado escribiendo y hablando sobre seguridad cibernética desde 1995. Es el analista jefe de investigación de IT-Harvest, la firma que fundó en 2005 para cubrir la floreciente industria de seguridad de TI. Es autor de *Surviving Cyberwar* (Government Institutes, 2010) y de *UP* y de *RIGHT: Strategy and Tactics of Analyst Influence* (IT-Harvest Press, 2012). Es frecuentemente citado como un experto en seguridad cibernética en los medios de comunicación tradicionales. Asesora a sus clientes en la estrategia de ciberseguridad. También es el Editor Ejecutivo de *securitycurrent.com* y el Senior Fellow en el *International Cybersecurity Dialogue*. Fue director de marketing de Fortinet, Inc. y vicepresidente de investigación de amenazas en Webroot Software. Anteriormente, fue Vicepresidente de Investigación en Gartner, Inc. Stiennon presentó amenazas y defensas de seguridad cibernética en 28 países en seis continentes. Es conocido por su análisis iconoclasta de la industria de la seguridad y siempre desafía a su audiencia a cuestionar las prácticas aceptadas frente a las amenazas cibernéticas cambiantes. Tiene una licenciatura en ingeniería aeroespacial y una maestría en Guerra en el mundo moderno de King's College, Londres. Está escribiendo su próximo libro sobre ciber guerra y asuntos militares. Su último libro es *Secure Cloud Transformation: The CIO's Journey*.



www.deletetechnology.com



email: marketing@deletetechnology.com
Tel: + (52) 55 4627 4100



Av. Ejército Nacional 826-A, Polanco
Miguel Hidalgo, CP 11540, CDMX.