



IRON
MOUNTAIN®

REPLANTEANDO LA ELIMINACIÓN DE ACTIVOS: ERRORES A EVITAR

POR: BROOKS HOFFMAN

Puede que también tu empresa haya adquirido teléfonos u ordenadores portátiles de segunda mano y los haya encontrado llenos de información personal de sus anteriores propietarios.

O hayas leído que organizaciones gigantes de todo el mundo han recibido multas millonarias por gestionar mal sus activos informáticos.

O has visto noticias muy preocupantes sobre vertederos en países en desarrollo que están repletos de productos electrónicos desechados, lo que ha devastado las regiones en las que se encuentran y ha proporcionado objetivos atractivos para los ciberdelincuentes, que saben que entre la basura hay información valiosa que se puede recoger fácilmente.

Mientras que la adquisición de activos informáticos suele ser el gran objetivo de cualquier estrategia empresarial basada en la tecnología, lo que ocurre cuando esos activos informáticos llegan al final de su vida útil, pero aún contienen información sobre la vida de la empresa y sus clientes, a menudo se ha tratado más bien como algo secundario.

Replantar la eliminación de activos informáticos (RAEE) y hacerla más prioritaria es fundamental a medida que los ciclos de los productos se acortan, la tecnología evoluciona a un ritmo vertiginoso y más empresas recurren a los servicios en la nube. Tendrás que ocuparte de una cantidad cada vez mayor de activos informáticos al final de su vida útil, y deberías tomar las decisiones correctas sobre vuestra estrategia RAEE para limitar el riesgo empresarial y proteger el medio ambiente.

RESIDUOS ELECTRÓNICOS: EL FLUJO DE RESIDUOS QUE MÁS CRECE

En todo el mundo, generamos unos 53 millones de toneladas de residuos electrónicos (e-waste) cada año, una cantidad que se prevé que se duplique con creces para el año 2050, según las Naciones Unidas. Esto hace que los residuos electrónicos sean el flujo de residuos que más rápido crece en el mundo. Las tecnologías de la información (no sólo en lo que se refiere al consumo de energía, sino al propio hardware) son ahora una parte importante de nuestra huella medioambiental. Y además es tóxica: los metales pesados (mercurio, plomo, cadmio y otros) pueden filtrarse de estos dispositivos al ecosistema, causando una amplia gama de problemas. No es de extrañar que cada vez más países se nieguen a aceptar más residuos electrónicos. Tailandia fue el último país en rechazarlos desde septiembre de 2020.





SEGURIDAD Y DESAFÍOS LEGALES

Los residuos electrónicos también plantean problemas inmediatos de seguridad y legales. Unos 25 estados, más el Distrito de Columbia, han adoptado leyes que exigen algún nivel de reciclaje de productos electrónicos, y han establecido sanciones para cuando el proceso se gestiona mal. Ontario (Canadá) ha empezado a aplicar una nueva normativa sobre residuos electrónicos, con el objetivo de alcanzar una tasa de reciclaje del 70%. Y hay muchas leyes y reglamentos de protección y privacidad de datos que tienen efectos de gran alcance en la eliminación de activos informáticos, incluida la legislación internacional. Por ejemplo, las empresas que entran en el ámbito de aplicación del Reglamento General de Protección de Datos (RGPD) se enfrentan a severas multas por incumplimiento, que pueden llegar a ser de hasta 20 millones de euros o el 4% de los ingresos globales anuales, en función de la gravedad y las circunstancias de la infracción.

ERRORES TÍPICOS DE LA GESTIÓN DE RAEE

Es esencial contar con procedimientos claros para una gestión de RAEE segura, pero es fácil cometer errores. He aquí algunos errores comunes que hay que evitar.

SIMPLIFICAR DEMASIADO.

Muchas empresas consideran que deshacerse del hardware informático obsoleto es una tarea sencilla: basta con limpiar los dispositivos y tirarlos a la basura. Por desgracia, no es tan sencillo. Los entresijos del borrado, la destrucción y la desmagnetización requieren procedimientos probados y eficiencia operativa. El simple hecho de borrar, reformatear o reiniciar puede no eliminar realmente los datos. Si los datos no se desinfectan correctamente o si los soportes no se destruyen adecuadamente, sigue existiendo el riesgo de una filtración de datos.

DEJAR LA GESTIÓN DE RAEE AL DEPARTAMENTO INFORMÁTICO

Aunque asignar la responsabilidad de la gestión de RAEE a tu personal de TI puede parecer lógico, no es necesariamente el caso. El proceso de eliminación segura de los equipos informáticos tiene aspectos técnicos, legales, logísticos y administrativos para los que tu departamento informático puede no tener los conocimientos necesarios, entre otros:

- > La coordinación con las personas y los departamentos que dependen de esos datos y los dispositivos que han llegado al final de su vida útil
- > Aplicar los procedimientos específicos necesarios para borrar completamente los datos existentes
 - Evaluar si la cadena de custodia (el seguimiento de quién ha tenido acceso a los dispositivos y cuándo lo ha hecho) se está capturando con precisión
 - Evaluar las credenciales medioambientales y de seguridad de los datos de un proveedor externo

Está claro que el departamento informático tiene un papel que desempeñar, pero también lo tienen otros administradores, departamentos y la alta dirección.

SUBESTIMAR VUESTRA RESPONSABILIDAD LEGAL.

A medida que aumenta la cantidad de residuos electrónicos, también lo hacen las leyes y normativas que los regulan, así como las multas por incumplimiento. Un proveedor de servicios financieros fue multado recientemente con 60 millones de dólares por gestionar mal el desmantelamiento de dos centros de datos. Y no es ni mucho menos el único que ha pagado multas.

No solo hay que preocuparse por las leyes y normativas que rigen específicamente los residuos electrónicos. Como se ha señalado anteriormente, los residuos electrónicos también entran en el ámbito del RGPD, de las normas del sector como PCI-DSS, de las leyes estatales de privacidad como la Ley de Privacidad del Consumidor de California (CCPA) y de normativas más amplias como HIPAA, la Ley MEGABYTE y Sarbanes-Oxley (SOX).

CONFIAR EN UN SERVICIO GRATUITO.

Hay empresas que ofrecen servicios de gestión de RAEE de forma gratuita o a un precio muy bajo, normalmente alegando que cubren sus costes mediante la reventa de tus dispositivos. Como en todas las cosas, se obtiene lo que se paga. Confiar en un proveedor de gestión de RAEE gratuito o de muy bajo coste no es una excepción a esta regla y es probable que el proveedor del servicio haga una o más de las siguientes cosas:

- Quedarse importantes ingresos obtenidos por el reciclaje de tus equipos, por lo que el servicio no es gratuito en absoluto
- Escatimar en aspectos como la seguridad de la cadena de custodia o la verificación completa de la destrucción de los datos en todos los dispositivos.
- Deshacerse de los equipos de forma irresponsable con el medio ambiente (por ejemplo, enviándolos al extranjero o vertiéndolos en los vertederos de nuestro país).

En resumen, puede que estés ahorrando dinero a muy corto plazo, pero estás poniendo en riesgo tu negocio y contribuyendo a los mismos impactos ambientales negativos que el reciclaje pretende evitar.

IGNORAR LA CADENA DE CUSTODIA.

Puede que no asocies intuitivamente un concepto legal como la cadena de custodia con la gestión de RAEE, pero es realmente la clave para hacerlo bien. Tanto si gestionas el RAEE por tu cuenta como si confías en un tercero, necesitarás un registro completo de dónde y a quién han ido a parar tus activos informáticos para establecer que tu gestión de RAEE ha sido realmente responsable y conforme, tanto desde el punto de vista medioambiental como de la seguridad de los datos. Además, las prácticas seguras de la cadena de custodia tienen una ventaja añadida: disuaden de los robos. El robo de dispositivos durante la gestión de RAEE puede ser un problema grave. Cuanto más pequeño y valioso sea un artículo, más probable es que desaparezca, y es menos probable que los ladrones intenten robar un activo que saben que está siendo rastreado.

Estos son todos los fallos que pueden hacer tropezar incluso a la organización más bien intencionada. Pero el mayor de todos es hacer que la eliminación de los activos informáticos al final de su vida útil sea algo secundario.

En su lugar, piensa que es una parte crítica del ciclo de vida continuo de gestión de la información, esencial para proteger tu información sensible y el medio ambiente.

Brooks Hoffman es miembro del equipo de Gestión de Productos del servicio de Eliminación Segura de Activos Informáticos ("SITAD") de Iron Mountain. Antes de incorporarse a Iron Mountain, fue cofundador y director financiero de LifeSpan, una empresa de eliminación de activos informáticos con sede en Denver, Colorado.

900.22.23.24 IRON | [IRONMOUNTAIN.ES](https://www.ironmountain.es)

QUIÉNES SOMOS

Iron Mountain Incorporated (NYSE: IRM), fundada en 1951, es el líder mundial en servicios de almacenamiento y gestión de la información. Con la confianza de más de 220,000 organizaciones en todo el mundo, y con una red de centros de más de 85 millones de pies cuadrados en más de 1,400 instalaciones en más de 50 países, Iron Mountain almacena y protege miles de millones de activos de información, incluida información comercial crítica, altamente sensible datos y artefactos culturales e históricos. Al proporcionar soluciones que incluyen almacenamiento seguro, gestión de la información, transformación digital, destrucción segura, así como centros de datos, almacenamiento de arte y logística, y servicios en la nube, Iron Mountain ayuda a las organizaciones a reducir costos y riesgos, cumplir con las regulaciones, recuperarse de desastres y Permitir una forma de trabajo más digital. Visita www.ironmountain.es para más información.

© 2021 Iron Mountain Incorporated. Todos los derechos reservados. Iron Mountain y el diseño de la montaña son marcas registradas de Iron Mountain Incorporated en los Estados Unidos y otros países. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios.