

Los cuatro pilares que sustentan la estrategia de ITAD: seguridad, sostenibilidad, escalabilidad y ahorro

Los riesgos para la seguridad de los datos, incluidas las brechas que les afectan, son noticia casi a diario. Los costes de las filtraciones aumentaron un 13 % entre 2020 y 2022, según IBM.¹ Con unos costes promedio de 4,35 millones de dólares en todo el mundo en 2022 (9,9 millones en Estados Unidos), cualquier incidente te puede penalizar, tanto desde el punto de vista financiero como del reputacional.

La eliminación de activos informáticos (ITAD) es una parte importante de la gestión de riesgos para la seguridad de los datos, y es algo que las organizaciones suelen pasar por alto. Una mala gestión del hardware obsoleto puede exponer datos corporativos confidenciales y dar lugar a la imposición de multas y sanciones por parte de las autoridades. A pesar de los riesgos asociados a la retirada de hardware, un nuevo estudio de Foundry revela que muchas empresas descuidan la adopción de medidas de seguridad adecuadas. Más del 40% de las empresas encuestadas aún no cuenta con una estrategia concreta de ITAD.

Estas cifras demuestran que, para mayor riesgo de la seguridad de los datos y de la reputación de las empresas, el interés por la ITAD es, a menudo, algo secundario. Al igual que el propietario de una vivienda que no piensa en la fontanería hasta que las tuberías se estropean, pocas personas se acuerdan de la ITAD hasta que tiene lugar un hecho que les perjudica.

Ha llegado el momento de plantear las cosas de otro modo. Las organizaciones deben empezar a reconocer la ITAD como una práctica estratégica que garantiza la seguridad de los datos, favorece la sostenibilidad, permite la escalabilidad y ahorra dinero. En este informe, analizaremos los cuatro pilares de la ITAD -seguridad, sostenibilidad, escalabilidad y ahorro-, y exploraremos los retos y oportunidades que suponen para las organizaciones.

EL ESTADO ACTUAL (A MENUDO INSEGURO) DE LA ITAD

La eliminación inadecuada de activos informáticos puede tener consecuencias nefastas. Si cae información sensible en las manos equivocadas, puede provocar pérdidas económicas, el robo de activos de propiedad intelectual y daños irreparables a la reputación de una organización. Pero si bien es fundamental asegurarse de que los activos retirados

Metodología del estudio

Foundry entrevistó a 405 decisores con responsabilidad en TI, gestión de activos, infraestructura de centros de datos/ TI, seguridad y cumplimiento normativo, compras y gestión de ESG, para conocer las prácticas, factores determinantes, retos y ventajas de la ITAD. Los encuestados procedían de seis países: **Estados Unidos, Reino Unido, Francia, Alemania, Países Bajos, Singapur y Australia**. El tamaño medio de las empresas era de 16.498 empleados.

se gestionan correctamente, el estudio de Foundry descubría que muchas organizaciones emplean numerosos métodos de destrucción de dispositivos que no son seguros. De hecho, muchas empresas no consideran que la eliminación segura de activos sea una prioridad para el negocio y no comprenden su grado de importancia y trascendencia.

Los encuestados admitieron llevar a cabo, con frecuencia u ocasionalmente, múltiples prácticas inseguras, entre ellas (ver gráfico 1):

- El 56% tira los activos a la basura con frecuencia u ocasionalmente.
- El 79% almacena activos obsoletos en sus instalaciones con frecuencia u ocasionalmente.
- El 58% almacena activos obsoletos fuera de las instalaciones con frecuencia u ocasionalmente

Sólo el 24% de los encuestados afirmó que destruía sus activos físicamente con regularidad. Los estadounidenses son más propensos a hacerlo (30%) que sus homólogos de Europa, Oriente Medio y África (21%), así como de Singapur y Australia (23%).

Es más, sólo el 44% de los encuestados reconoció destruir o limpiar de manera habitual los datos de los activos informáticos que se desecharan.

Pero ¿por qué? Muchos consideran que el riesgo de sanear los equipos informáticos es mayor que el beneficio que se obtiene con ello. Casi la mitad (45%) afirmó que borrarlos o eliminarlos de forma inadecuada supone un riesgo mayor que dejarlos intactos.

Otros motivos son:

- 28% - falta del conocimiento o de las habilidades necesarias
- 24% - falta de la tecnología necesaria
- 22% - falta de presupuesto

LOS RETOS DE LA ITAD: ¿QUÉ SE INTERPONE EN SU CAMINO?

La mayoría de los departamentos de TI saben y admiten que realizar un seguimiento de dónde se encuentran los dispositivos informáticos (por ejemplo, los portátiles) es un gran desafío.

Gráfico 1

Cómo gestionan las organizaciones los activos obsoletos

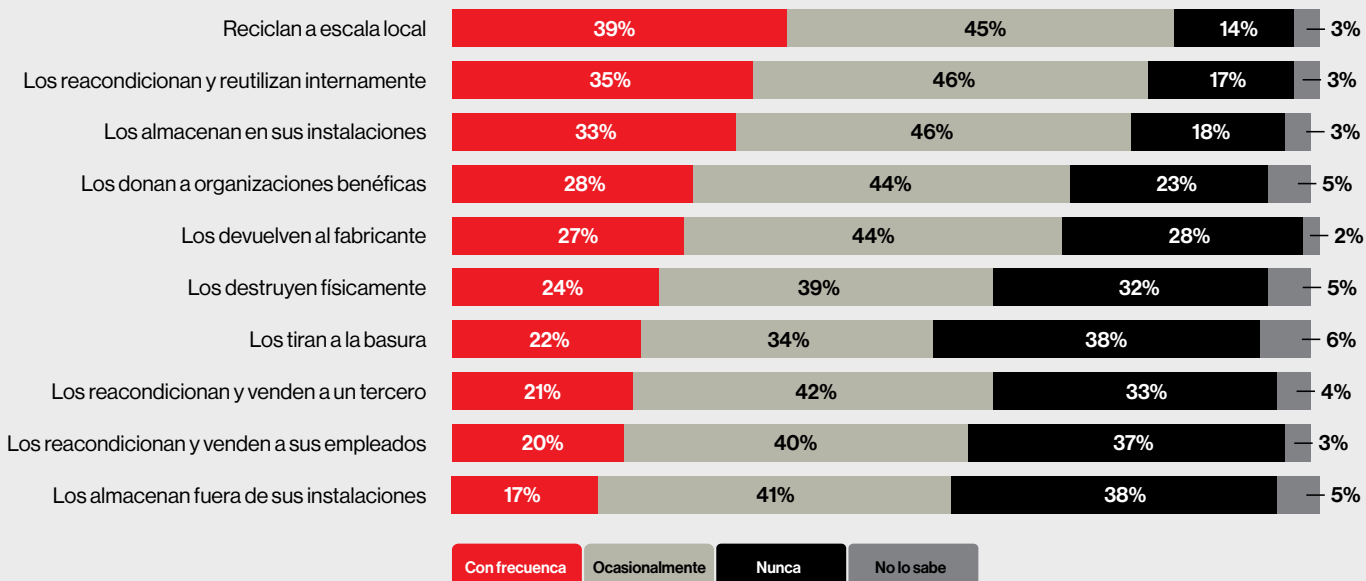
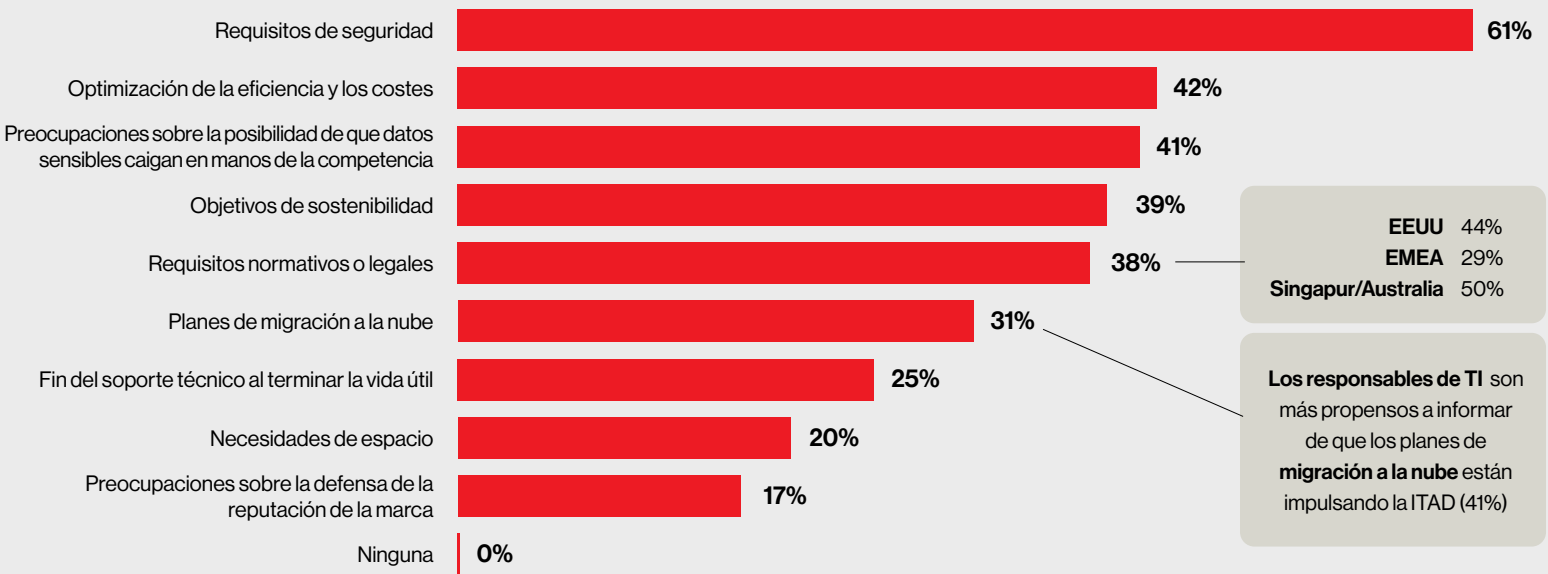


Gráfico 2

Principales motivaciones para aplicar una estrategia de ITAD



Fuente: Foundry

De hecho, el estudio de Foundry revela que el 45% de los responsables de TI afirman estar preocupados por la gestión y el seguimiento de los activos informáticos a lo largo de todo su ciclo de vida. Otra gran preocupación es el seguimiento de los dispositivos que se encuentran en múltiples localizaciones (33%). Conocer la propiedad o la ubicación exacta de los dispositivos remotos plantea retos aún mayores cuando los empleados trabajan a distancia o cuando abandonan una organización.

Los departamentos de TI tienen dificultades para gestionar los equipos de los trabajadores que trabajan en remoto porque, a menudo, carecen de información precisa sobre el inventario. Esto se refleja en las respuestas de la encuesta, ya que los usuarios consultados señalaron que cada vez hay más activos fuera del control del departamento de TI (41%), y que se devuelven más dispositivos debido a la alta rotación (40%).

Cuando se les preguntó por los aspectos más problemáticos de una estrategia ITAD, el 39% de los encuestados citó el cumplimiento de los requisitos normativos y de seguridad. Otros puntos candentes fueron la cadena de custodia (28%), la falta de recursos (28%) y los datos incompletos (27%). Los responsables de TI son conscientes de los riesgos que conlleva no implantar un programa de ITAD, pero son conscientes de

las ventajas de hacerlo. Los requisitos de seguridad son una de las principales motivaciones de la estrategia de ITAD para más de la mitad de los entrevistados (61%).

LOGRAR LOS OBJETIVOS DE SOSTENIBILIDAD GRACIAS A LA ITAD

Los residuos electrónicos constituyen una de las áreas de más rápido crecimiento en el ámbito de los residuos sólidos y representan un importante desafío para las iniciativas de sostenibilidad. Al mismo tiempo, las empresas se ven obligadas a replantearse y mejorar sus programas de sostenibilidad para responder a las crecientes expectativas y objetivos de clientes y grupos de interés. La ITAD puede desempeñar un papel importante a la hora de resolver el problema del exceso de residuos electrónicos y cumplir con los objetivos de sostenibilidad.

Hay buenas y malas noticias en lo que respecta a las prácticas sostenibles de ITAD. El 39% de las organizaciones reciclan activos informáticos y el 35% los reacondiciona y reutiliza internamente. Son cifras esperanzadoras. En comparación, el 35% de los encuestados recicló activos informáticos y el 31% los reutilizó, según una encuesta de 2020 realizada por Foundry y Iron Mountain. Este último sondeo también reveló que el 22% de los encuestados admite tirar con

frecuencia a la basura sus activos informáticos, mientras que el 24% los destruye físicamente.

Quienes gestionan la ITAD de forma centralizada afirman estar más seguros de que los equipos de hardware se manejan de forma segura y ecológica (el 71% expresa una gran confianza, frente al 59% de los que llevan a cabo una gestión descentralizada). Las empresas que quieran comprometerse con objetivos de sostenibilidad pueden beneficiarse de un socio ITAD de confianza que cuente con un largo historial de aplicación de las mejores prácticas, como maximizar la reutilización, maximizar el reciclaje de aquello que no pueda reutilizarse y minimizar las emisiones de CO2 y los residuos electrónicos. También es importante preguntar a los potenciales proveedores si cumplen con las normas del sector, como los Reales Decretos que legislan en España la gestión de RAEE (aparatos eléctricos y electrónicos).

CÓMO EL TRABAJO REMOTO HA CAMBIADO LA ESCALA DE LA ITAD

El tamaño y el alcance de una estrategia de ITAD también pueden presentar retos ante la generalización de las políticas de trabajo híbrido o remoto. A medida que aumenta el número de activos tecnológicos ubicados fuera de las instalaciones de la empresa, su eliminación segura resulta más costosa, compleja y difícil.



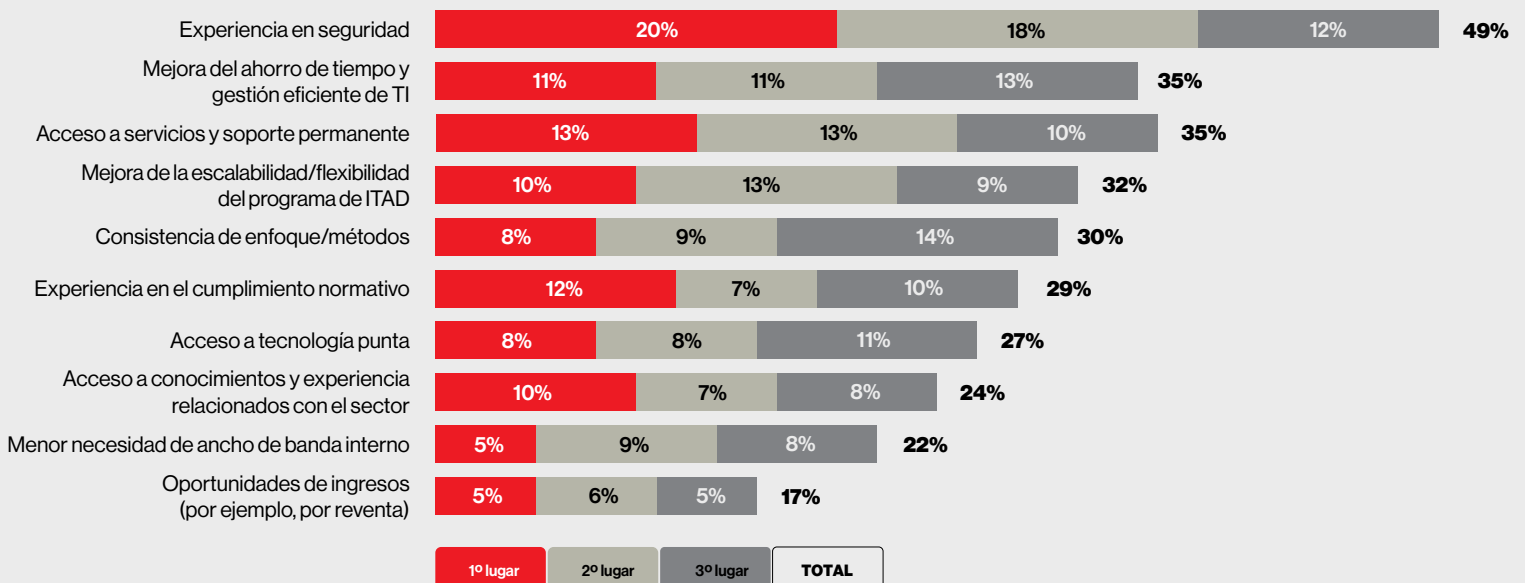
La actual era del trabajo híbrido, unida a una mano de obra activa que cambia de empresa con frecuencia, presenta varios retos emergentes para la ITAD. El 41% afirma que el número de activos fuera del control corporativo ha aumentado. Entre sus problemas emergentes destacan:

- 40% - aumento del volumen de activos devueltos debido a la elevada rotación de personal
- 29% - falta de medios seguros para que los trabajadores a distancia devuelvan los equipos.

Ante la enorme cantidad de equipos informáticos que hay que supervisar, no es de extrañar que las organizaciones necesiten ayuda. Los responsables de TI se plantean solicitar la ayuda de una estrategia de ITAD por muchas razones, pero la primera es aprovechar la experiencia en seguridad de un proveedor, tal y como menciona el 49% de los encuestados (ver gráfico 3).

Gráfico 3

Principales beneficios potenciales de contar con un proveedor de ITAD



VALORAR EL AHORRO MEDIANTE LA ITAD

La mayoría de las empresas se centran en frenar los costes. La eliminación de dispositivos informáticos no es una excepción: el 44% de los encuestados cita el ahorro de costes como la principal razón para desarrollar una estrategia de ITAD. Además, aquellos que la han implementado se están dando cuenta de los ahorros, con un 47% que lo señala como un beneficio clave.

Los responsables de TI que cuentan con un programa formal de ITAD perciben varios beneficios adicionales. Casi la mitad (49%) ha experimentado una mejora en la seguridad y la privacidad de los datos. Otras ventajas son la mayor consistencia de las prácticas de gestión de TI en todas las sedes (40%) y el cumplimiento de los objetivos corporativos de sostenibilidad (36%).

UN SOCIO DE CONFIANZA CUMPLE CON LOS CUATRO PILARES DE LA ITAD

Un programa de ITAD moderno debe centrarse en la seguridad de los datos en torno a los equipos informáticos que se desechan. Esto requiere una capacidad escalable para limpiar los dispositivos que contienen datos, hacer un seguimiento desde su recogida hasta su eliminación final y proporcionar un registro que certifique que los datos y los equipos se han eliminado correctamente.

Un programa de ITAD de primera clase también favorece la sostenibilidad. Para garantizar la sostenibilidad de un programa de ITAD, las empresas deben trabajar con un proveedor que cuente con las certificaciones necesarias en todo momento.

Las razones para desarrollar e implantar un programa formal de ITAD son evidentes. Iron Mountain lleva más de 70 años gestionando datos y archivos para la empresa y es tu aliado para la eliminación segura, sostenible y flexible de activos de TI, garantizando que minimizas el riesgo y maximizas el valor de los equipos informáticos al final de su vida útil. ♦

→ **Contacta con Iron Mountain para saber cómo**

te podemos ayudar a alcanzar tus objetivos de seguridad y sostenibilidad mediante un programa de ITAD

www.ironmountain.com/itad

