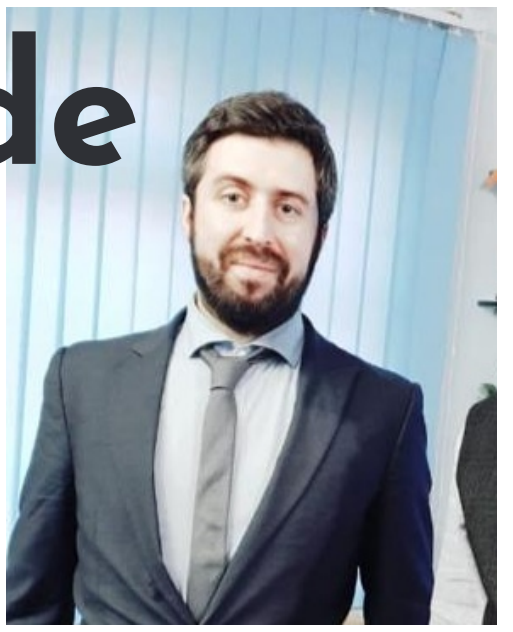
07 Destrucciónde Datos



Davide Maddalozzo

Business Development Manager tecnología.

ProDevice

¿Qué rol juega la destrucción de datos en la ciberseguridad?

En los últimos años, ha habido muchas preocupaciones asociadas con la comunidad moderna de ciberseguridad. El rol de la ciberseguridad dentro de las organizaciones, se ha vuelto crucial para la postura financiera y la reputación de cada empresa e institución.

Cuando los líderes de las organizaciones piensan en la ciberseguridad, la atención se centra principalmente en las herramientas y prácticas que se implementarán para mejorar la protección de la estructura cibernética actual.

Todos se defienden contra los robos y el robo de datos mediante el uso de varios firewall robustos, antivirus, soluciones de almacenamiento en la nube, seguridad de redes y endpoints, capacitación de concientización para los empleados, hasta las tecnologías de aprendizaje automático e inteligencia artificial más recientes.

Lo que generalmente no se considera, o se subestima, es qué hacer cuando es necesario retirar o desechar los portadores de medios y los endpoints.

Para la postura de seguridad de una organización, es fundamental proteger los datos durante toda su vida útil, lo que incluye qué hacer con los datos cuando ya no son necesarios.

Millones de smartphones, discos y varios soportes electrónicos obsoletos, no utilizados, rotos o defectuosos se tiran diariamente a la basura, después de un simple formateo, o se fríen en hornos de microondas, o se rompen con un martillo en la creencia de que esto es suficiente.

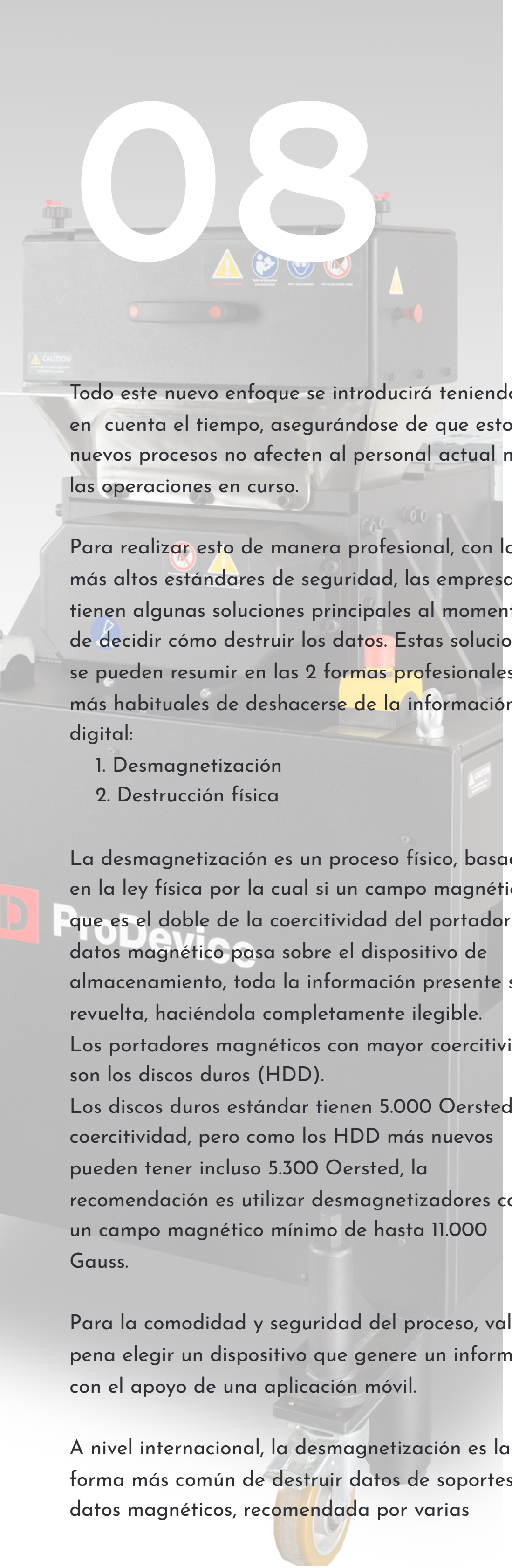
Estos datos aún se pueden recuperar y utilizar con éxito. Y esto es exactamente lo que conduce a fugas masivas de datos, violaciones del RGPD, robos, chantajes, ventas de datos confidenciales, desastres de relaciones públicas, escándalos.

Tal y como explica el Instituto Nacional de Ciberseguridad del Gobierno de España: “Las empresas, independientemente de su tamaño o de su sector, basan su actividad en la información. El ciclo de vida de la información, de forma simplificada, consta de tres fases: generación, transformación y destrucción.

Toda información tiene una vida útil, ya sea en formato digital o en formatos tradicionales. Cuando la vida de los documentos llega a su fin, se deben utilizar mecanismos de destrucción y borrado para evitar que queden al alcance de terceros."

Por lo tanto, las organizaciones deben implementar un paso adicional para garantizar que nadie pueda leer ni acceder a los datos antes de su eliminación.

El primer paso a considerar es un nuevo enfoque de la política de retención de datos, creando auditorías y procesos internos para determinar los tipos de hardware que se utilizan para almacenar datos y cuándo se debe destruir un soporte de datos específico.



08

Destrucción de Datos

Todo este nuevo enfoque se introducirá teniendo en cuenta el tiempo, asegurándose de que estos nuevos procesos no afecten al personal actual ni a las operaciones en curso.

Para realizar esto de manera profesional, con los más altos estándares de seguridad, las empresas tienen algunas soluciones principales al momento de decidir cómo destruir los datos. Estas soluciones se pueden resumir en las 2 formas profesionales más habituales de deshacerse de la información digital:

1. Desmagnetización
2. Destrucción física

La desmagnetización es un proceso físico, basado en la ley física por la cual si un campo magnético que es el doble de la coercitividad del portador de datos magnético pasa sobre el dispositivo de almacenamiento, toda la información presente será revuelta, haciéndola completamente ilegible.
Los portadores magnéticos con mayor coercitividad son los discos duros (HDD).
Los discos duros estándar tienen 5.000 Oersted de coercitividad, pero como los HDD más nuevos pueden tener incluso 5.300 Oersted, la recomendación es utilizar desmagnetizadores con un campo magnético mínimo de hasta 11.000 Gauss.

Para la comodidad y seguridad del proceso, vale la pena elegir un dispositivo que genere un informe, con el apoyo de una aplicación móvil.

A nivel internacional, la desmagnetización es la forma más común de destruir datos de soportes de datos magnéticos, recomendada por varias asociaciones de ciberseguridad y protección de datos, como la tecnología más segura, fácil de usar, que ahorra tiempo y es más efectiva.

Alternativamente, o en combinación con la desmagnetización, es posible destruir físicamente los diferentes soportes, perforando con destructores manuales profesionales y certificados o triturando con trituradores de medios automáticos.

La destrucción de los soportes, así como la norma de seguridad, está regulada y categorizada por la norma internacional DIN66399, que divide el proceso en 7 niveles de seguridad diferentes, 3 categorías de protección y 6 clasificaciones de materiales.

El uso de estas tecnologías profesionales y su implementación dentro de la política de ciberseguridad de la organización beneficiará a la empresa en muchos niveles.

En primer lugar la responsabilidad, ya que los clientes, socios y empleados tendrán la seguridad de que la información confidencial no caerá en manos no autorizadas o criminales después de la disposición de los portadores.

Además, es importante tener en cuenta que el RGPD europeo, así como la mayoría de los Reglamentos locales de protección de datos más recientes y las guías y estándares internacionales (como CCPA, HIPPAA, NIST, ISO27001) se refieren claramente a la destrucción de datos y cómo, cuándo y por qué se deben destruir los datos confidenciales y desechar los soportes de datos.

Las mismas guías requieren mantener un registro de sus actividades de eliminación de datos, especialmente datos confidenciales y de alto riesgo. Si haces el proceso internamente o si decides hacerlo a través de una empresa que ofrece servicios de destrucción de datos onsite y offsite, será importante generar el informe y certificado de destrucción de datos al finalizar el servicio.

La selección del dispositivo o marca adecuada deberá incluir las especificaciones técnicas adecuadas y la capacidad de ese producto para generar un informe profesional y confirmar la eficiencia del proceso.

Teniendo en cuenta las obligaciones de la mayoría de las empresas de adherirse a las normas y reglamentos anteriores, puede ser necesario adoptar métodos y tecnologías efectivos para mantener el pleno cumplimiento.

Una consideración sobre los beneficios debe incluir la conciencia de que la mayoría de los clientes y socios se están volviendo extremadamente conscientes de la importancia de la protección de datos y de todos los riesgos relacionados con una ciberseguridad insuficiente.

Una violación de datos o una pérdida de datos no es solo un gran problema económico y financiero, sino también un daño a la reputación que puede dirigir a los clientes potenciales a empresas competidoras, que pueden ofrecer soluciones más modernas y efectivas.

Recuerde que puede ser más seguro y económico a largo plazo invertir en la eliminación segura que arriesgarse a perder datos confidenciales sobre tu empresa, lo que podría costarte mucho más, sin incluir demandas judiciales y multas si se han perdido datos personales del consumidor.

Recuerda, los discos duros se pueden reemplazar, pero ¿tu reputación? Difícilmente.

La destrucción de datos es protección de datos. Be aware, choose wisely.