



SECTOR
ITAD'S



NORMAS Y REGLAMENTOS QUE APLICAN EN EL SECTOR

- Reglamento General de Protección de Datos (GDPR) de la UE
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (INAI, México).
- Ley 1581-2012 Ley de Protección de Datos en Colombia
- Ley General de Protección de Datos Personales (LGPD) de Brasil
- Ley Orgánica de Protección de Datos Personales (LOPD) de Ecuador
- Ley No. 29733 de Protección de Datos Personales de Perú
- Ley 19.628 de Protección de Datos de Chile
- Ley Orgánica 3/2018 Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) de España
- Estándar establecido por la National Association for Information Destruction (NAID)
- ADISA (Asset Disposal & Information Security)
- R2V3 es una actualización del Estándar R2 (Responsible Recycling)
- e-Stewards

SOLUCIONES PARA EL BORRADO SEGURO Y PERMANENTE DE LA INFORMACIÓN



¿QUÉ ES BLANCCO?

Blancco ofrece una gama de soluciones para el borrado de información a nivel físico, lógico y virtual. El borrado seguro más el reporte 100% auditable que genera **Blancco** es la evidencia necesaria para el cumplimiento normativo en México y Latinoamérica. Al establecerse como el estándar mundial en borrado de datos certificado, **Blancco** ha sido probado, certificado y recomendado por 19 organismos oficiales, autoridades legales y laboratorios de pruebas.





SECTOR ITAD's

ESTÁNDAR ESTABLECIDO POR LA NATIONAL ASSOCIATION FOR INFORMATION DESTRUCTION (NAID)

La certificación **NAID AAA** establece varios requerimientos clave para asegurar el borrado seguro de información:

- 1. Seguridad del Proceso:** Las empresas deben implementar procedimientos estrictos para la destrucción de datos, asegurando que toda la información sea eliminada de manera irreversible.
- 2. Seguridad de las Instalaciones:** Las instalaciones donde se realiza la destrucción de datos deben estar protegidas contra accesos no autorizados.
- 3. Procedimientos de Destrucción de Datos:** Se deben utilizar métodos aprobados para la destrucción de datos, como la desmagnetización, la destrucción física y la sobrescritura.
- 4. Políticas de Contratación Segura:** Los empleados deben pasar verificaciones de antecedentes para asegurar que no tengan antecedentes penales relacionados con el robo de información.
- 5. Auditorías Regulares:** Las empresas certificadas deben someterse a auditorías anuales, tanto programadas como no anunciadas, para verificar el cumplimiento continuo de los estándares.

Estos requerimientos aseguran que las empresas certificadas por **NAID AAA** manejen y destruyan la información de manera segura y conforme a las regulaciones más estrictas.

R2V3 ES UNA ACTUALIZACIÓN DEL ESTÁNDAR R2 (RESPONSIBLE RECYCLING)

La Norma R2V3 establece varios requerimientos específicos para asegurar el borrado seguro de infor-

mación en dispositivos electrónicos. Aquí te detallo los principales:

- 1. Evaluación de Riesgos:** Las empresas deben realizar una evaluación de riesgos para identificar los tipos de datos que manejan y determinar los métodos más adecuados para su eliminación segura.
- 2. Métodos de Borrado Aprobados:** Se deben realizar métodos de borrado que se garanticen la destrucción completa de los datos. Estos métodos incluyen la sobrescritura, la desmagnetización y la destrucción física de los dispositivos.
- 3. Verificación del Borrado:** Después de realizar el borrado, es necesario verificar que los datos han sido eliminados de manera irreversible. Esto puede incluir pruebas de recuperación de datos para asegurar que no se pueda acceder a la información eliminada.
- 4. Documentación y Registro:** Las empresas deben mantener registros detallados de todos los procesos de borrado de datos, incluyendo los métodos utilizados, las fechas y los resultados de las verificaciones.
- 5. Auditorías y Cumplimiento:** Las empresas certificadas deben someterse a auditorías periódicas para asegurar el cumplimiento continuo de los estándares de la Norma R2v3.

Estos requerimientos aseguran que las empresas manejen y destruyan la información de manera segura y conforme a las regulaciones más estrictas, protegiendo así la confidencialidad y la integridad de los datos.

DIFERENCIADORES

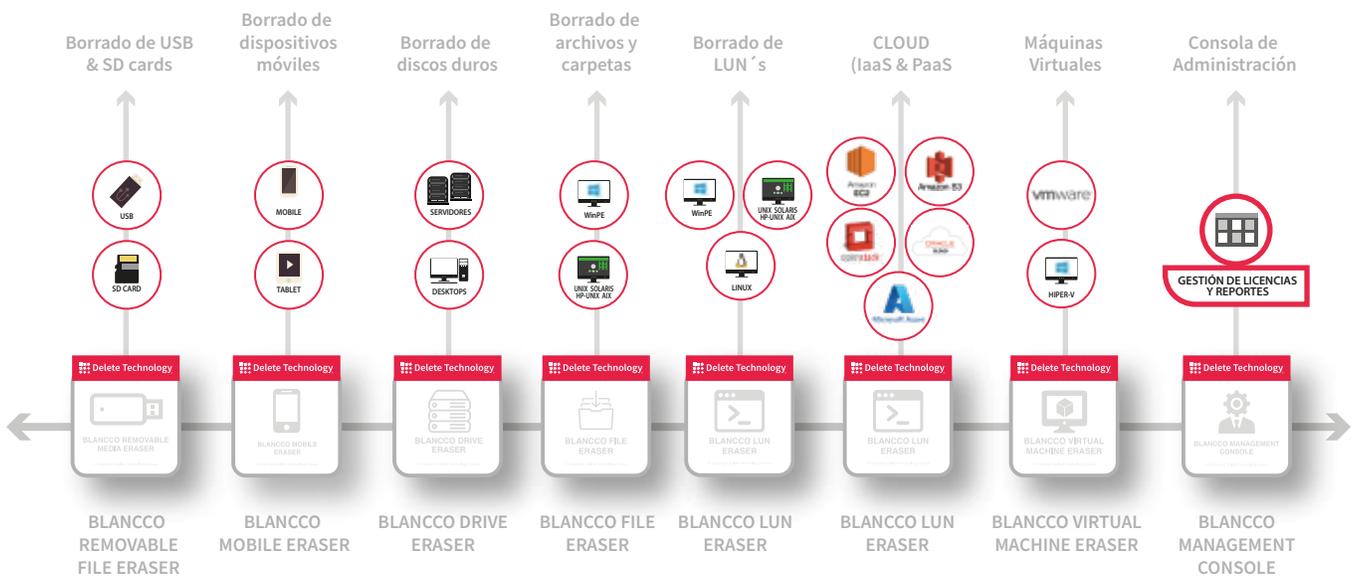
Reporte Auditable

En sistemas operativos (SO) actuales, típicamente hay dos opciones para realizar un borrado: un formateo y un formateo rápido. El formateo rápido no es una solución segura porque sólo remueve los índices, pero un formato completo, intenta sobrescribir el espacio en disco disponible para el SO con ceros. Si todo resulta perfecto, se eliminarán grandes extensiones de datos. Sin embargo, en la realidad el nivel de detalle que se necesita para asegurar un borrado seguro es más complejo. El problema con el formateo tradicional es que no hay forma de confirmar que los datos han sido borrados permanentemente. La verificación y certificación de Blancco (ver reporte) son procesos clave para la seguridad y auditoría de la información.



Conformidad de Funcionalidad
Funcionalidad
Adaptabilidad
De acuerdo a la Guía de Borrado de
Seguro de Datos Personales
publicada por el INAI

BORRADO SEGURO Y CERTIFICADO DE INFORMACIÓN



© Copyright Delete Technology Group S.A de C.V 2024

Delete Technology Group S.A de C.V
Av. Ejército Nacional 826A Oficina 104 Col. Polanco CDXM 11540 México

DELETETECHNOLOGY, el logotipo de DELETETECHNOLOGY son marcas comerciales de DELETE TECHNOLOGY S.A. DE C.V., registradas en muchas jurisdicciones del mundo. Otros nombres de productos y servicios pueden ser marcas comerciales de DELETE TECHNOLOGY o de otras empresas. En la web se encuentra disponible una lista actualizada de las marcas comerciales de DELETE TECHNOLOGY, en "Copyright and trademark information",

Este documento está actualizado hasta la fecha inicial de publicación y puede ser modificado por DELETETECHNOLOGY en cualquier momento. No todas las ofertas se encuentran disponibles en todos los países en que DELETETECHNOLOGY opera. Los datos de rendimiento y ejemplos de clientes que se citan se presentan solo a título ilustrativo. Los resultados de rendimiento reales pueden variar en función de las configuraciones y condiciones operativas específicas.

LA INFORMACIÓN EN ESTE DOCUMENTO ES PROPORCIONADA "COMO ES", SIN NINGUNA GARANTÍA, YA SEA EXPLÍCITA O IMPLÍCITA, Y SIN NINGUNA GARANTÍA DE COMERCIALIZACIÓN, ADECUACIÓN PARA UN PROPÓSITO EN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO CONTRAVENCIÓN.

Los productos DELETE TECHNOLOGY están garantizados de acuerdo con los términos y condiciones de los acuerdos en virtud de los cuales se proporcionan. El cliente es responsable de asegurarse del cumplimiento de las leyes y normas que sean de aplicación. DELETE TECHNOLOGY no proporciona asesoramiento legal ni declara o garantiza que sus productos o servicios asegurarán que el cliente cumpla alguna ley o norma determinada. Las declaraciones en cuanto a futuras direcciones y propósitos de DELETE TECHNOLOGY están sujetas a cambios o cancelaciones sin previo aviso y solo representan metas y objetivos.

www.deletetechnology.com.mx