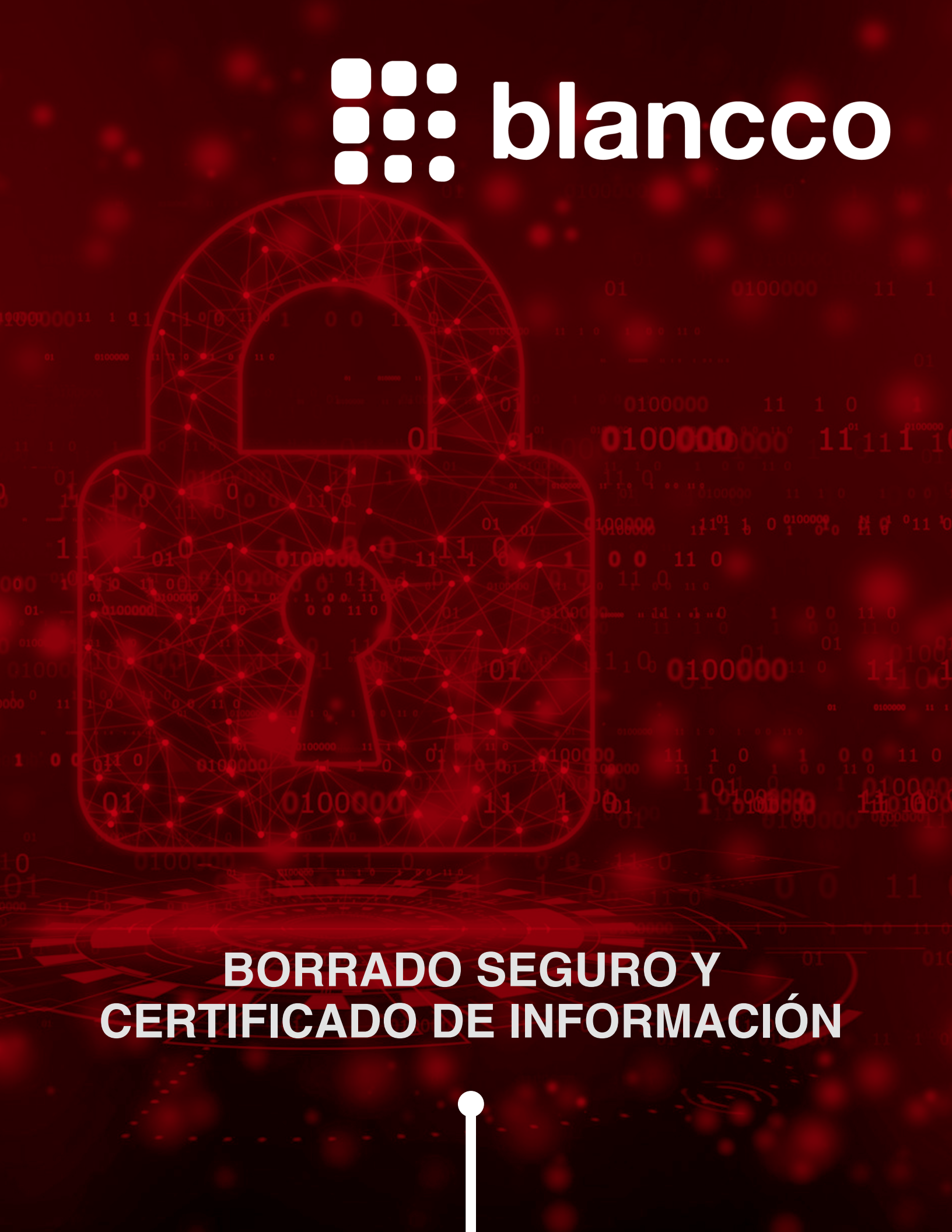
blancco



BORRADO SEGURO Y CERTIFICADO DE INFORMACIÓN

¿EL BORRADO DE DATOS ES REALMENTE SEGURO?

Cuando se trata de salvaguardar la información confidencial, las organizaciones no pueden permitirse el lujo de cortar atajos. La **destrucción** completa de datos en dispositivos de almacenamiento de datos cuando llegan al final de su vida útil es esencial para cualquier estrategia de **protección de datos corporativa**. Para muchas organizaciones, esto significa enviar unidades a través de una trituradora.

Si bien este tipo de destrucción física es ciertamente valioso en cualquier política de seguridad de TI, no siempre es la mejor opción. Sí, triturar la mayoría de las unidades tradicionales hará que los datos sean irrecuperables, pero se ha descubierto que la destrucción de las tecnologías más nuevas, como las **SSD**, deja datos en los fragmentos de la unidad, creando la posibilidad de una violación de datos mientras la unidad queda inutilizable.

El **borrado seguro** y certificado de datos se ha convertido en una opción popular para las organizaciones que desean deshacerse de los registros de datos confidenciales. El borrado de datos puede agregar seguridad adicional a un proyecto de destrucción física. También se puede utilizar como el único medio para eliminar datos de unidades, teléfonos móviles, medios extraíbles y más.

¿Pero es el borrado de datos lo suficientemente seguro como para reemplazar la destrucción física?

LIMITACIONES DE LA DESTRUCCIÓN FÍSICA

Para explorar las credenciales de seguridad de la eliminación de datos basada en software, primero debemos observar las limitaciones de la destrucción física. La destrucción física ha sido un incondicional de la industria para la historia del hardware de TI, particularmente para las unidades de disco duro. Pero no es la única opción, y con frecuencia no la mejor, para los datos altamente confidenciales almacenados en los tipos de unidades más nuevos. Los **SSD** y otros activos de TI pueden destruirse físicamente de protección segura de datos.

con fuerza bruta, pero debido a la forma cada vez más densa en que se almacenan los datos, los chips intactos y los datos que contienen pueden permanecer en fragmentos de hardware triturado. Esta vulnerabilidad, más los gastos de reemplazo de unidades, puede ser costosa para las empresas.

También es costoso para el medio ambiente. A medida que el movimiento "verde" gana impulso y la tecnología global necesita un aumento vertiginoso, existe preocupación por el rápido consumo de recursos naturales para nuevos dispositivos, así como por la gran cantidad de dispositivos usados (desechos electrónicos) que van a los vertederos. Dadas estas dos preocupaciones por la destrucción física, las organizaciones están observando más de cerca sus resultados y su papel en la sostenibilidad, manteniendo estrictos estándares.

El **borrado de datos** proporciona esa seguridad al sobrescribir los datos en toda la unidad, incluidas las áreas **HPA / DCO** y los sectores defectuosos, verificando que los datos son irrecuperables y proporcionando documentación a prueba de manipulaciones que las unidades han sido desinfectadas completamente. Además, los estándares respetados de desinfección de datos y los líderes de la industria han validado el borrado de datos como una opción segura de protección de datos al final de la vida útil, ya sea solo o junto con la destrucción física de datos altamente confidenciales.

¿CÓMO FUNCIONA EL BORRADO DE DATOS?

El **borrado de datos basado en software sobrescribe los datos en cualquier dispositivo de almacenamiento,** reemplazando los datos originales con ceros y unos. Todos los sectores del dispositivo sobrescriben por completo, con la opción de realizar sobrescrituras múltiples donde las regulaciones lo exijan. Una vez que se completa este proceso, los datos en el dispositivo son completamente irrecuperables por cualquier medio forense, lo que permite la reutilización del dispositivo si lo desea. El **borrado de datos** logra la desinfección completa de datos según lo definido por el Consorcio Internacional de **Sanitización de Datos y Gartner.**

Una gama de estándares modernos de cumplimiento de la gobernanza de datos ahora incluye el borrado de datos como un método preferido de desinfección de datos. Aunque estándares como DoD y NIST recomiendan diferentes números de pases de sobrescritura, ambos validan que la sobrescritura basada en software es una forma segura de eliminación de datos. Muchas empresas utilizan el borrado de datos basado en software para agregar una capa adicional de seguridad a su proceso de disposición de activos de TI.

Cuando los activos alcanzan el final de su vida útil, se pueden desinfectar completamente con el borrado de datos antes de realizar la destrucción física, lo que significa que no se pueden recuperar datos residuales de los fragmentos después del hecho. Esta **seguridad** adicional permite a las organizaciones dedicarse a sus negocios con el conocimiento reconfortante de que están protegidas contra el acceso no autorizado a datos al desmantelar activos.

Copyright © 2019 Blancco Technology Group. All Rights Reserved.

Delete Technology® blancco team NYCE Seguridad y Confianza PCI DSS Certified bsi.

Y no son solo los activos de TI al final de la vida los que cosechan los beneficios de la eliminación de datos basada en software. Las empresas también pueden borrar datos dentro de entornos activos, de forma segura y certificable, sin tiempo de inactividad. El cumplimiento es clave en cualquier negocio que almacene información de identificación personal. Muchas regulaciones, incluidas GDPR e HIPAA, estipulan que las empresas deben deshacerse de los datos en entornos activos una vez que haya pasado su fecha de retención.

Blancco es el **líder de la industria en el borrado seguro de datos** basado en software.

Ofrecemos un conjunto de soluciones de borrado para desinfectar completamente cualquier activo de TI en entornos activos y al final de su vida útil, creando un registro de auditoría a prueba de manipulaciones que demuestra el cumplimiento de una gama de normas, estándares y pautas globales.

Obtenga más información sobre cómo el borrado de datos puede beneficiar a su organización en nuestro documento técnico gratuito.

"Protección de datos empresariales: lo que necesita saber para proteger los datos corporativos durante su ciclo de vida".

" **Data sanitización** es el proceso disciplinado de eliminar o destruir de forma deliberada, permanente e irreversible los datos almacenados en un dispositivo de memoria para que sea irrecuperable".

"Gartner"