Protocolos de Seguridad Digital

abka

Nuestro Compromiso con la Seguridad de la Información en Impresoras

En abka Colombia, la seguridad de la información es una prioridad fundamental en todos nuestros procesos y servicios. Reconocemos que las impresoras y equipos multifuncionales modernos son potenciales puntos de vulnerabilidad si no se administran adecuadamente, ya que manejan y almacenan datos sensibles de nuestros clientes.

Por esta razón, hemos desarrollado un conjunto integral de protocolos de seguridad diseñados específicamente para fortalecer la protección de los datos en nuestras impresoras, tanto durante su operación normal como al finalizar su ciclo de servicio. Estos protocolos abarcan dos aspectos críticos: el borrado seguro de datos y el hardening o robustecimiento de las configuraciones de seguridad.

Protocolo de borrado seguro de datos

1. Habilitación y configuración de sobrescritura segura.

Todas las impresoras de abka Colombia deben tener habilitado y configurado el Sistema *DataOverwriteSecurity (DOSS)* para sobrescribir de forma segura los datos temporales del disco duro al finalizar cada trabajo de impresión, copia, escaneo o fax.

2. Definición de ciclos de sobrescritura según criticidad

La cantidad de ciclos de sobrescritura del DOSS se debe configurar entre 1 a 9 pasadas, según el nivel de criticidad de los datos manejados por cada impresora y siguiendo las recomendaciones de la NSA/DoD.

3. Monitoreo del proceso de sobrescritura

Los administradores de las impresoras deben monitorear periódicamente el icono DOSS para asegurar que el proceso de sobrescritura se ejecute exitosamente.

4. Borrado seguro al retirar impresoras de servicio

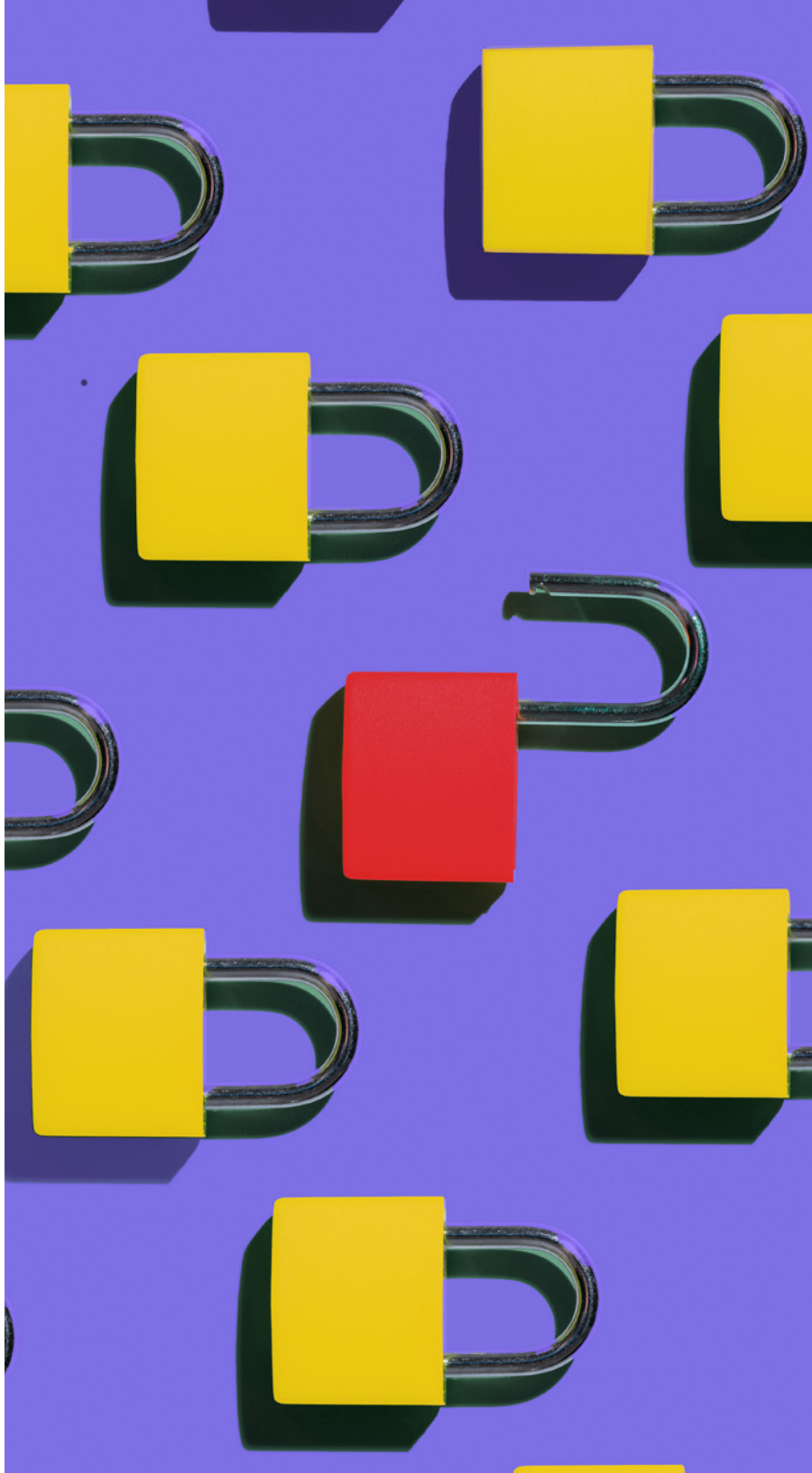
Al retirar una impresora de servicio en abka Colombia, ya sea por traslado, finalización de contrato o reemplazo, se debe ejecutar un servicio de sobreescritura completa del disco duro siguiendo los estándares de la NSA/DoD. Adicionalmente, se debe inicializar la memoria NV-RAM a valores predeterminados para eliminar datos como direcciones IP, libretas de direcciones, etc.

5. Manejo de discos duros retenidos por clientes

En caso que un cliente de abka Colombia requiera retener el disco duro de una impresora al finalizar su servicio, un técnico certificado deberá extraer el disco antes que el equipo abandone las instalaciones del cliente. El disco extraído se transferirá bajo custodia a un representante autorizado del cliente, quien será responsable de destruir los datos por el método que considere apropiado.

6. Limpieza de impresoras antes de su retiro

Todo equipo de impresión de abka Colombia que vaya a ser retirado de las instalaciones de un cliente deberá someterse a un servicio de limpieza que incluya: borrado de datos almacenados (libretas de direcciones, configuraciones de red, etc.), remoción de etiquetas con información sensible (nombres, IPs) y material impreso confidencial olvidado en bandejas o cassettes.



Protocolo de hardening de impresoras

1. Actualización controlada de firmware

El firmware de todas las impresoras en abka Colombia debe mantenerse actualizado con las últimas versiones liberadas por el fabricante. Solo se instalarán versiones firmadas digitalmente para asegurar su integridad. El proceso de actualización se realizará de forma automática usando la herramienta Device Manager NX.

2. Autenticación de usuarios y control de acceso

Todas las impresoras tendrán habilitada autenticación de usuarios para permitir el acceso solo a personal autorizado. Se implementarán métodos como autenticación Windows/LDAP, códigos PIN o tarjetas de acceso según el entorno del cliente. Los permisos de acceso se otorgarán de forma granular en base a roles y grupos de usuarios predefinidos.

3. Encriptación de discos duros

Los discos duros de las impresoras en abka Colombia contarán con encriptación AES de 256 bits para proteger los datos almacenados, incluyendo libretas de direcciones, datos de autenticación, documentos, registros, etc.

4. Aseguramiento de puertos de red y desactivación de protocolos inseguros

Durante la configuración inicial de cada impresora, los técnicos de abka Colombia deshabilitarán todos los puertos de red innecesarios, dejando abiertos solo aquellos requeridos. Adicionalmente, se desactivarán protocolos inseguros que no estén en uso, como Telnet, FTP o SNMPv1

5. Cifrado de comunicaciones de red

Todas las comunicaciones de red de las impresoras, incluyendo tráfico de impresión, administración y monitoreo, serán encriptadas usando protocolos SSL/TLS. Para conexiones inalámbricas se habilitará WPA2 con cifrado AES-CCMP.

6. Capacitación en seguridad para usuarios y administradores

abka Colombia brindará capacitación recurrente a usuarios y administradores de sus impresoras, para asegurar que conozcan las funcionalidades de seguridad disponibles, su configuración apropiada y las mejores prácticas para mantener un entorno de impresión seguro.


abka