Un enfoque integral para la seguridad de las impresoras.

Las impresoras y los equipos multifunción tienen ahora la capacidad de trabajar en el centro de sus operaciones comerciales. Con el crecimiento exponencial de los dispositivos inalámbricos, el software y los servicios alojados en la nube, sus impresoras no solo necesitan trabajar con estas nuevas tecnologías, sino que también deben protegerse de ellas.

PROTECCIÓN INTEGRAL PARA SU IMPRESORA

En Xerox, desde hace mucho tiempo reconocimos y aceptamos el cambio en la tecnología y las necesidades cambiantes del lugar de trabajo. Ofrecemos un conjunto integral de funciones de seguridad que mantienen sus impresoras y datos a salvo. Además, protegemos cada parte de la cadena de datos, incluidos **la impresión, la copia, el escaneado, el fax, la descarga de archivos** y **el software del sistema.** Son cuatro los aspectos más importantes de nuestro enfoque de varios niveles.

PREVENIR

La primera y más obvia vulnerabilidad es la interfaz de usuario, así como mantener el control sobre quiénes tienen acceso físico a su impresora y sus funciones. Las medidas de seguridad de Xerox empiezan con la prevención de intrusiones mediante la **Autenticación de usuarios** para asegurar que solo personal autorizado tenga acceso. Una vez ahí, el **Control de acceso basado en roles** asegura que cada miembro del equipo solo vea las funciones que usted quiera que vea. La habilitación de **Contraseñas fuertes y complejas** protege contra los piratas informáticos y el software malicioso, y la compatibilidad con la **autenticación de múltiples factores**[1] proporciona un nivel adicional de seguridad. También se registran todas las acciones relacionadas con cada usuario, lo que proporciona un registro completo de **Auditoría**.

Enseguida, abordamos los puntos de intrusión menos obvios: lo que se envía a la impresora y la forma en que se envía. Nuestro software del sistema está **firmado digitalmente**: cualquier intento de instalación de versiones infectadas y sin firmar hará que el archivo se rechace automáticamente. Las claves cifradas se almacenan en los chips del TPM, lo que mantiene a las impresoras protegidas contra ataques cibernéticos.

xerox™

DETECTAR

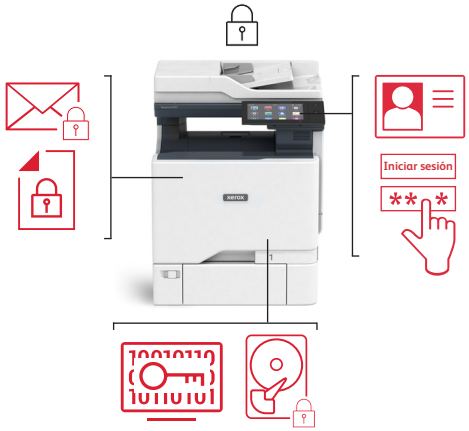
En el improbable caso de que las defensas de sus datos y su red se vean superadas, la tecnología Xerox® ConnectKey® ejecuta un **análisis de verificación de firmware** completo, bien al arranque o cuando lo activa un usuario autorizado. Se dará una alerta si se detectan cambios dañinos a la impresora. Nuestras soluciones integradas más avanzadas usan la tecnología de **listas de permitidos de Trellix**[2], que realiza una supervisión constante y previene automáticamente la ejecución de cualquier software malintencionado. La integración con el **Motor de servicios de identidad (ISE) de Cisco®** detecta automáticamente los dispositivos Xerox® en la red y los clasifica como impresoras a fin de lograr la implementación y el cumplimiento de las políticas de seguridad. Los dispositivos Xerox® se integran con las herramientas de software SIEM[3] líderes del mercado para comunicar los datos de eventos de seguridad en tiempo real. Esto ayuda en la detección anticipada de violaciones y elimina o mitiga el daño potencial de las amenazas de seguridad a la organización.

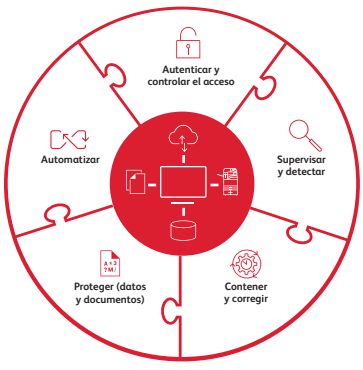
PROTEGER

Nuestras soluciones de seguridad integral protegen los documentos impresos y escaneados de su divulgación o modificación no autorizada. La tecnología Xerox® ConnectKey® ayuda a impedir la transferencia deliberada o accidental de datos clave a personas no autorizadas.

Protegemos los documentos impresos utilizando un **código PIN** o un sistema de **liberación mediante tarjetas**. Podemos evitar que la información escaneada llegue a personas que no deberían recibirla gracias a **formatos de archivos protegidos con clave, cifrados y firmados digitalmente**. Las impresoras con tecnología ConnectKey también le permiten **bloquear los campos de correo electrónico "para/cc/cco"** limitando los destinos de escaneado a las **direcciones internas**.

Además, protegemos toda la información almacenada mediante los niveles más altos de **cifrado**. Borramos cualquier dato procesado o almacenado que no se necesite mediante el uso de **algoritmos de limpieza** y **borrado de datos**[4] aprobados por el Instituto Nacional de Normas y Tecnología (NIST) y el Departamento de Defensa de los EE. UU.





XEROX ES COMPATIBLE CON LA CONFIANZA CERO

Con una combinación de hardware, software y procesos, respaldamos las iniciativas de Confianza cero (Zero Trust) para hacer que la implementación sea más sencilla y más integral.

Más información: www.xerox.com/es-ar/quienes-somos/soluciones-de-seguridad/seguridad-confianza-cero

ASOCIACIONES EXTERNAS

Trabajamos con organizaciones que realizan pruebas de conformidad y con líderes del sector de seguridad como **Trellix y Cisco** para adaptar sus estándares y conocimientos a los productos de Xerox.

Al compararnos con estándares internacionales, organismos de certificación como **Criterios comunes (ISO/ IEC 15408)** y **FIPS 140-2/ 140-3** brindan pruebas independientes de que cumplimos con los niveles más altos de rendimiento. Estos reconocen nuestro enfoque integral en la seguridad de la impresora.

Nuestro programa de corrección de errores (Bug Bounty)[5] con HackerOne es otra marca de confianza en nuestras medidas de seguridad, así como un recurso independiente de validación tecnológica.

Trellix · cisco · splunk> · LogRhythm · hackerone

SEGURIDAD FÁCIL DE IMPLEMENTAR Y GESTIONAR

Seleccione entre las plantillas de seguridad predefinidas (Predeterminada, Elevada o Alta) y la impresora configurará automáticamente los ajustes de seguridad correspondientes. Supervise hasta 75 ajustes de seguridad con el Control de configuración y los restablecerá automáticamente si se detectan cambios no autorizados. Esto ayuda al personal de TI a ahorrar tiempo y elimina las conjeturas a la hora de implementar y cumplir con las políticas de seguridad.

[1] La autenticación multifactor se habilita a través de Xerox® Workplace Solutions y los IdP en la nube

[2] Los dispositivos Xerox® AltaLink®, los equipos multifunción Xerox® VersaLink® C415 color/B415 y C625 color/B625, la impresora Xerox® VersaLink® C620 color/B620, el equipo multifunción Xerox® VersaLink® de la serie 7100 y el equipo multifunción Xerox® de la serie EC7800/8000

[3] Trellix Enterprise Security Manager, LogRhythm y herramientas SIEM Splunk

[4] Aplica solo a dispositivos con unidad de disco duro

[5] La corrección de errores (Bug Bounty) se ofrece a través de HackerOne en los equipos multifunción Xerox® AltaLink®, con la adición de más productos, soluciones y servicios en el futuro

Más información: **www.xerox.com/es-ar/quienes-somos/soluciones-de-seguridad**

 10/24 TSK-6323 BR40786 XOGFS-62LE

xerox™