Lexmark™
A Xerox Company



# Guía de referencia de seguridad de Lexmark



En materia de seguridad, su empresa debe garantizar la administración segura de sus impresoras de red, defenderlas de los piratas informáticos y proteger la información más importante. En Lexmark, hemos diseñado nuestros dispositivos para satisfacer las necesidades de seguridad únicas de su empresa, con las funciones de seguridad más avanzadas del sector.




# Enfoque en seguridad desde el diseño

Asegurar un entorno empresarial es complejo y requiere un conocimiento integral del software y el hardware, de la arquitectura de red, de los contenidos que circulan por ella, de los factores humanos, así como de la postura y los objetivos de seguridad de cada organización. También se necesitan conocimientos especializados para traducir los conceptos teóricos de seguridad en productos y servicios seguros.

Lexmark no deja la seguridad para el último momento ni la añade como una función opcional, sino que la considera un diseño integral y un objetivo de ingeniería, por lo que la incorpora en todos sus productos y servicios. De hecho, este enfoque sistemático de seguridad desde el diseño ofrece un beneficio clave a nuestros clientes: la confianza para gestionar su negocio de manera rentable, sabiendo que sus dispositivos y datos están protegidos en todo momento.

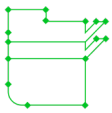
Nuestra comprensión de los entornos de red y de las amenazas de seguridad relevantes, especialmente en relación con la impresión, proporciona la experiencia necesaria para crear soluciones únicas que protegen sus datos en todos los niveles, una capacidad que hemos demostrado al trabajar y superar los desafíos de seguridad en algunas de las organizaciones e industrias más reguladas del mundo.

A diferencia de otros, somos dueños toda nuestra tecnología, incluidos el hardware, el firmware y el software. Esto significa que los expertos en desarrollo internos de Lexmark pueden trabajar con su organización con base en los requisitos específicos y reaccionar con rapidez y agilidad para satisfacer sus necesidades de seguridad.



# Proteja todas las facetas de la seguridad de impresión

La experiencia de Lexmark como líder del sector en seguridad de documentos y dispositivos constituye la columna vertebral de nuestra tecnología. Nuestro perfil de seguridad para productos y estándares, combinado con nuestro enfoque de seguridad desde el diseño, ayuda a los clientes a proteger su parque de impresoras con la oferta de seguridad más completa del sector, desde el primer momento.



Productos



Estándares



## Productos

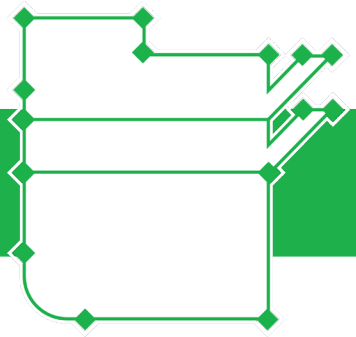
- Verificación y arranque seguro del sistema operativo
- Módulo de plataforma de confianza
- Protección de memoria y almacenamiento
- Protecciones de firmware
- Separación del fax y la red
- TLS 1.3
- Autenticación y autorización
- Acceso al dispositivo y a la configuración
- Seguridad incorporada de fábrica
- Borrado por retirada de servicio
- Registros de auditoría con syslog seguro
- Gestión de certificados
- Puertos y protocolos seguros
- PrintCryption

## Estándares

- Criterios Comunes (certificación NIAP/CCEVS, ISO 15408)
- FIPS 140-3 (cifrado)
- SOC2 tipo II (nube)
- ISO 20243 (cadena de suministro)
- ISO 27001 (información)
- NIST (normas)

Estas capacidades forman la base de un enfoque multicapa y multifacético para garantizar el más alto nivel de seguridad de los dispositivos y los datos a lo largo de todo el proceso de salida. Hemos integrado la seguridad en todos los dispositivos que producimos, desde las impresoras de sobremesa más pequeñas hasta nuestros equipos multifunción empresariales más grandes y todo lo que hay en medio. Esto significa que ya no tiene que elegir entre un dispositivo adecuado para su organización o uno seguro.

# Productos



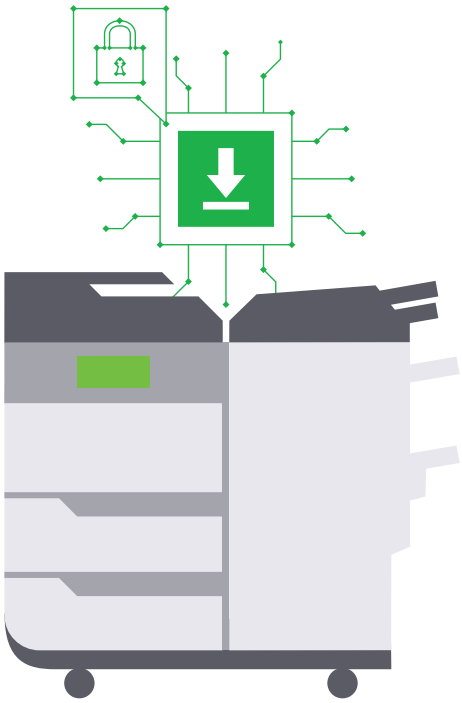
Mejore la seguridad de la impresora con hardware y firmware líderes del sector



# Dispositivo seguro

Las impresoras y los equipos multifunción de Lexmark proporcionan una sólida oferta de seguridad para proteger los puntos finales y reforzar el sistema. Nuestras capacidades avanzadas de seguridad permiten a los usuarios minimizar las amenazas y vulnerabilidades, al tiempo que optimizan su inversión tecnológica.

- **Tecnología de arranque seguro:** Los usuarios pueden verificar que el firmware instalado en la impresora sea auténtico de Lexmark; si se detecta firmware no original, el dispositivo mostrará una notificación de error.
- **Verificación continua:** Los administradores pueden garantizar que el firmware no se ha manipulado durante el funcionamiento. El código se valida nuevamente cada vez que se lee desde el almacenamiento persistente.
- **Firmware cifrado y firmado digitalmente:** Las impresoras y los equipos multifunción Lexmark inspeccionan automáticamente las actualizaciones de firmware descargadas en busca de las firmas digitales apropiadas de Lexmark. El firmware que no esté correctamente empaquetado y firmado por Lexmark es rechazado.



- **Integración de Active Directory:** La compatibilidad con Microsoft Active Directory se ofrece en dispositivos Lexmark compatibles con soluciones con pantalla táctil. El uso de Active Directory en la última generación de dispositivos con pantalla táctil de Lexmark es un método seguro de autenticación y autorización que facilita y agiliza la gestión de la seguridad de los dispositivos para los recursos de TI.
- **Autenticación mediante tarjeta con contacto y sin contacto:** Las soluciones de autenticación por credenciales incluyen soluciones de tarjeta de contacto y sin contacto para la autenticación básica. Esta opción está disponible cuando la identidad del usuario está vinculada a tarjetas de identificación de seguridad de oficina. Las soluciones pueden verificar la identificación de la tarjeta y recuperar la información del usuario, de modo que el dispositivo Lexmark pueda acceder a trabajos de impresión retenidos, identificar el origen de los documentos escaneados o reconocer al usuario para otros fines.



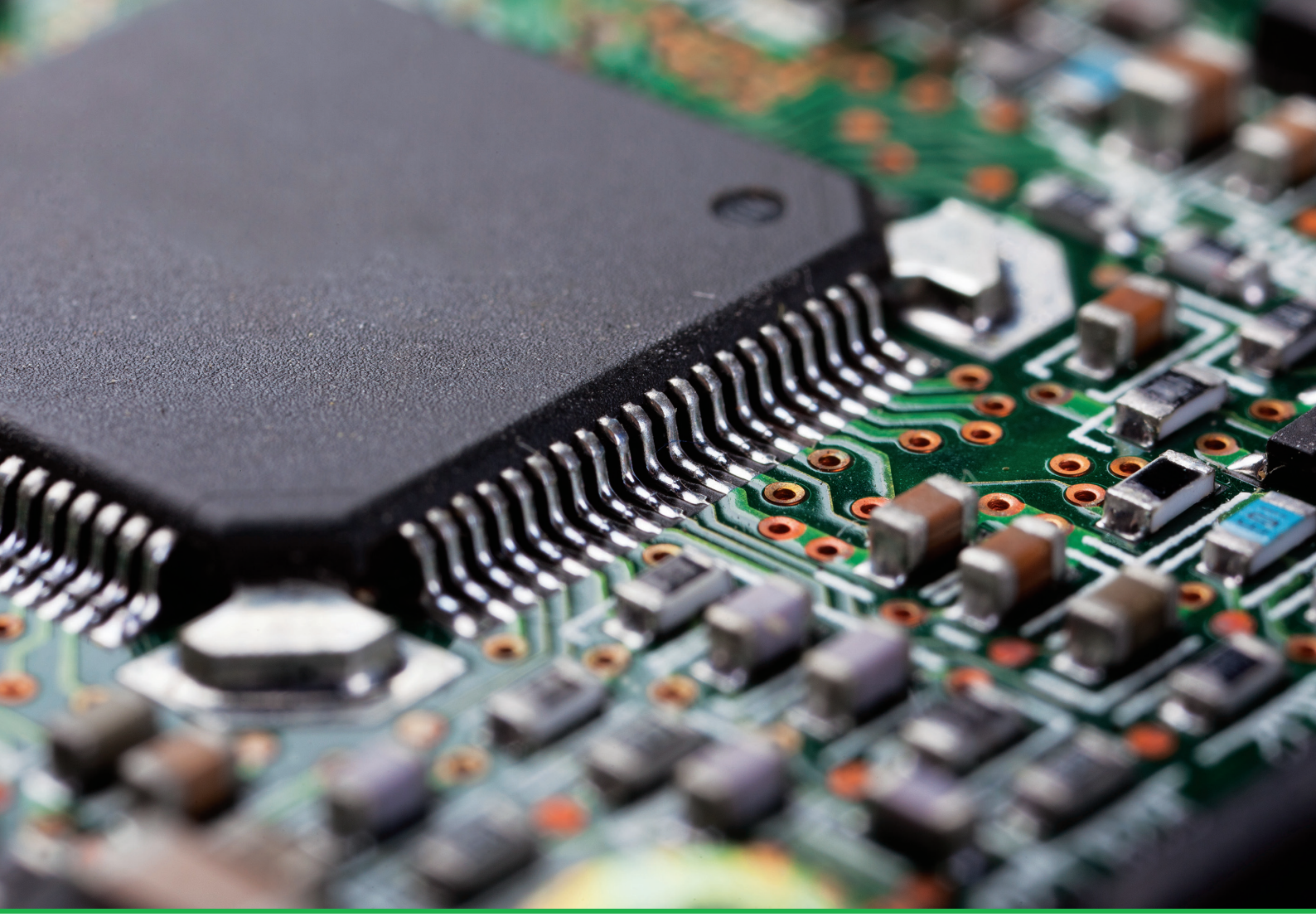
Todo el hardware, el software y el firmware de Lexmark se diseña mediante los principios de seguridad descritos en nuestro ciclo de vida de desarrollo de software seguro (SSDL). El proceso aborda todos los aspectos de la seguridad, desde la planificación hasta el diseño y la implementación, incluyendo el aseguramiento de la calidad, el lanzamiento y el mantenimiento, y ofrece puntos de control de protección inigualables para cumplir con los estándares de seguridad más exigentes de su organización.



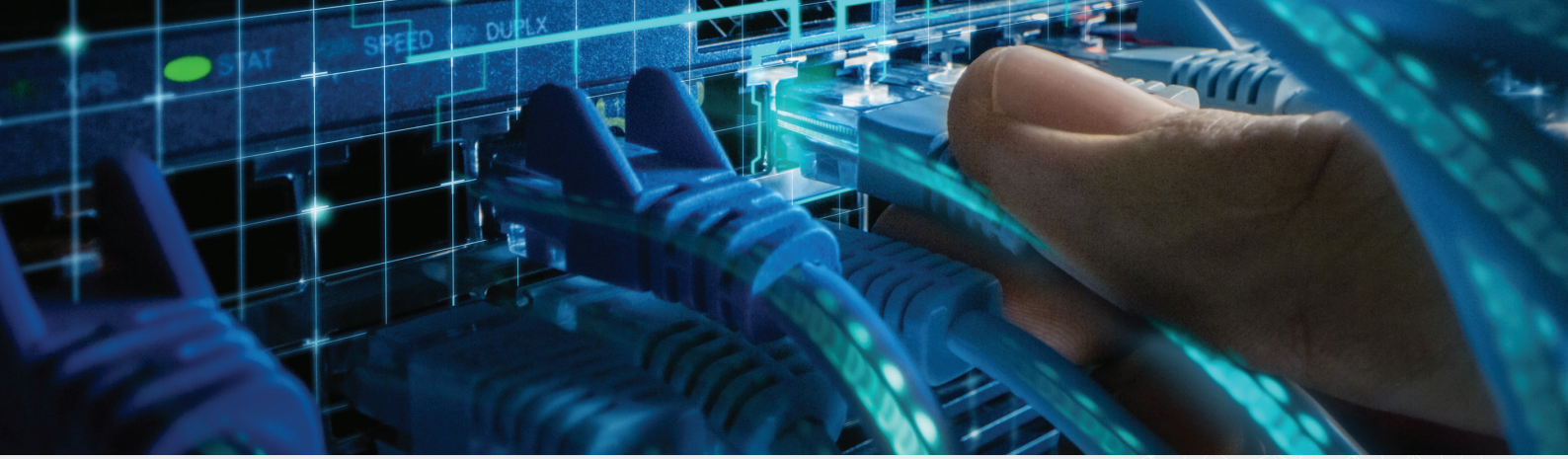
# Datos seguros

Los dispositivos Lexmark incorporan una amplia gama de características cuidadosamente diseñadas para mejorar la seguridad de los datos almacenados en el dispositivo y ayudar a evitar que usuarios malintencionados accedan a información confidencial.

- **Almacenamiento cifrado:** Actualmente hay varias ubicaciones para almacenar datos en impresoras y equipos multifunción, que se pueden configurar para utilizar el cifrado. La impresora o el equipo multifunción genera internamente una clave AES de hasta 256 bits y se usa para cifrar todos los datos. La clave se almacena en el dispositivo de forma no contigua, lo que permite acceder al contenido solo desde la impresora o el equipo multifunción original. Los datos de un componente robado no serían accesibles aunque se instalara en un modelo idéntico de impresora o equipo multifunción.
- **Limpieza del disco duro:** Los datos escritos en los discos duros de las impresoras o los equipos multifunción para uso temporal al imprimir, escanear, enviar faxes o copiar pueden borrarse cuando se completa el trabajo o después de imprimir un trabajo retenido para un usuario determinado. Para garantizar que la información nunca pueda recuperarse, los discos duros de las impresoras y los equipos multifunción de Lexmark eliminan tanto la referencia del archivo en el directorio del disco como el archivo real, de manera que no se puedan leer datos residuales. En función del dispositivo, el borrado del disco duro se puede configurar en modo manual, automático o programado. También se ofrece un borrado de múltiples pasadas que cumple con los estándares del Instituto Nacional de Estándares y Tecnología (NIST) y del Departamento de Defensa (DOD).
- **Borrado completo del disco:** Antes de retirar, reciclar o sacar una impresora o un equipo multifunción de un entorno seguro, un usuario autorizado puede borrar completamente la unidad. Esto incluye la eliminación de los formularios, las fuentes, las macros o los trabajos en espera todavía no impresos que un borrado de disco duro puede dejar atrás. Se ofrecen opciones de borrado de una sola pasada o de múltiples pasadas, que garantizan que no quede ningún dato legible en el disco.
- **Borrado de la memoria no volátil:** La limpieza de la memoria no volátil proporciona una herramienta para borrar todo el contenido almacenado en los distintos formatos de memoria flash incluidos en el dispositivo. Esta característica consiste en un borrado completo de todos los ajustes, las soluciones, los trabajos y los faxes del dispositivo.
- **Borrado por retirada del servicio:** Este proceso simplifica la eliminación de datos en todos los componentes de almacenamiento al retirar un dispositivo del servicio o sacarlo de una ubicación segura. Los usuarios autorizados pueden realizar ambas acciones en un solo paso mediante el comando de borrado por retirada del servicio, disponible en el menú de configuración del dispositivo o en su página web.



- **Módulo de plataforma de confianza:** A partir de los anuncios de productos de 2022, ahora se incluye un Módulo de plataforma de confianza (TPM) estándar que proporciona autenticación, verificaciones de la integridad del sistema y capacidades criptográficas para crear una huella digital única del sistema. El TPM se está convirtiendo rápidamente en el estándar del sector para la seguridad del hardware empresarial y proporciona una experiencia más segura para los usuarios al almacenar claves de cifrado del disco duro en una pieza de hardware independiente de los datos que cifra con capas de protección adicionales. Este hardware también contribuye a fortalecer el cifrado mediante la generación mejorada de números aleatorios.




# Red segura

Desde la desactivación de funciones innecesarias hasta el bloqueo de las interfaces del dispositivo y la protección de los datos que contienen, los dispositivos Lexmark incluyen una amplia gama de características integradas que refuerzan la seguridad frente a ataques.

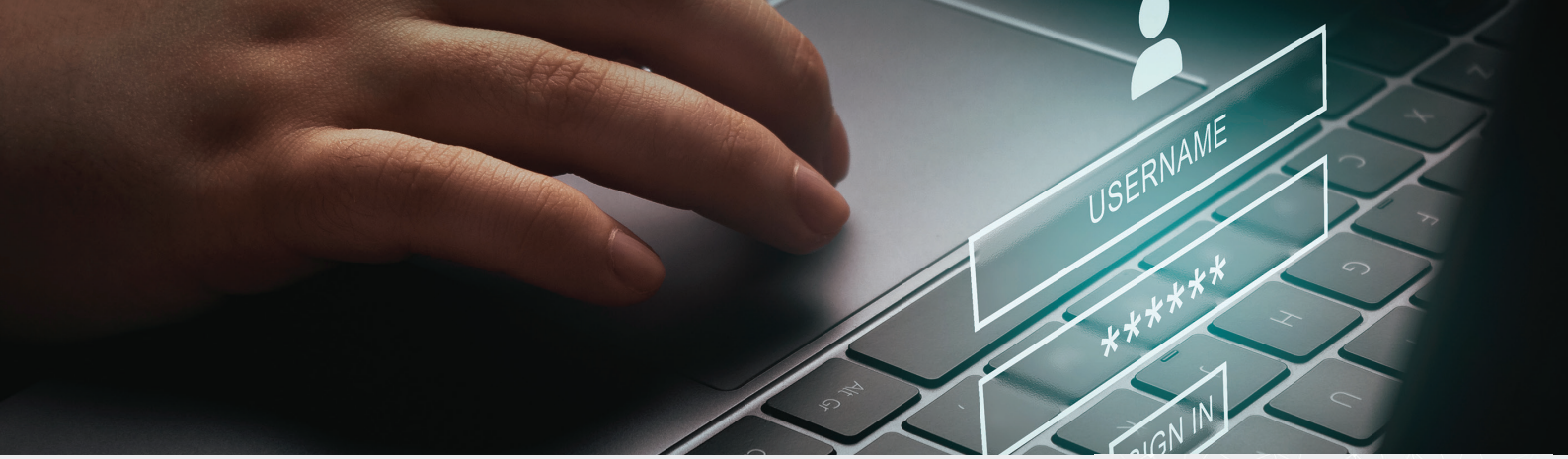
- **Filtrado de conexiones TCP:** Las impresoras y los equipos multifunción se pueden configurar para permitir conexiones TCP/IP únicamente desde una lista específica de direcciones TCP/IP, lo que protege el dispositivo frente a impresión o configuración no autorizadas.
- **Filtrado de puertos:** Los puertos de red a través de los cuales las impresoras y los equipos multifunción reciben o transmiten tráfico de red son configurables, lo que permite un alto grado de control sobre la actividad de red del dispositivo. Se pueden deshabilitar explícitamente puertos y protocolos de red como Telnet, FTP, SNMP, HTTP y otros.
- **802.1x:** Con la autenticación de puerto 802.1X, las impresoras y los equipos multifunción pueden conectarse a redes cableadas e inalámbricas, requiriendo que los dispositivos se autentiquen antes de acceder a la red.
- **IPSec:** La opción de protocolo IPsec, cuando está activada, protege el tráfico de red hacia y desde los dispositivos Lexmark mediante cifrado y autenticación. Esto garantiza la protección de los datos de impresión y del contenido de los trabajos que se escanean a cualquier destino.
- **LDAP seguro:** Todo el tráfico LDAP hacia y desde los dispositivos Lexmark se puede proteger mediante TLS. La información de LDAP, como credenciales, nombres y direcciones de correo electrónico, que se intercambia a través de una conexión TLS, se cifra para preservar la confidencialidad y la privacidad de los datos.



- **Seguridad incorporada de fábrica:** Seleccionar las opciones adecuadas para la configuración de seguridad de la impresora puede ser un reto. A partir del firmware 7, cuando los clientes optan por la seguridad incorporada de fábrica, existe la posibilidad de crear una cuenta de administrador, y el dispositivo desactivará muchos puertos y protocolos heredados no seguros y activará el cifrado del disco de forma predeterminada. Además, el asistente de configuración hace que la experiencia inicial con el dispositivo sea igual de sencilla que segura.



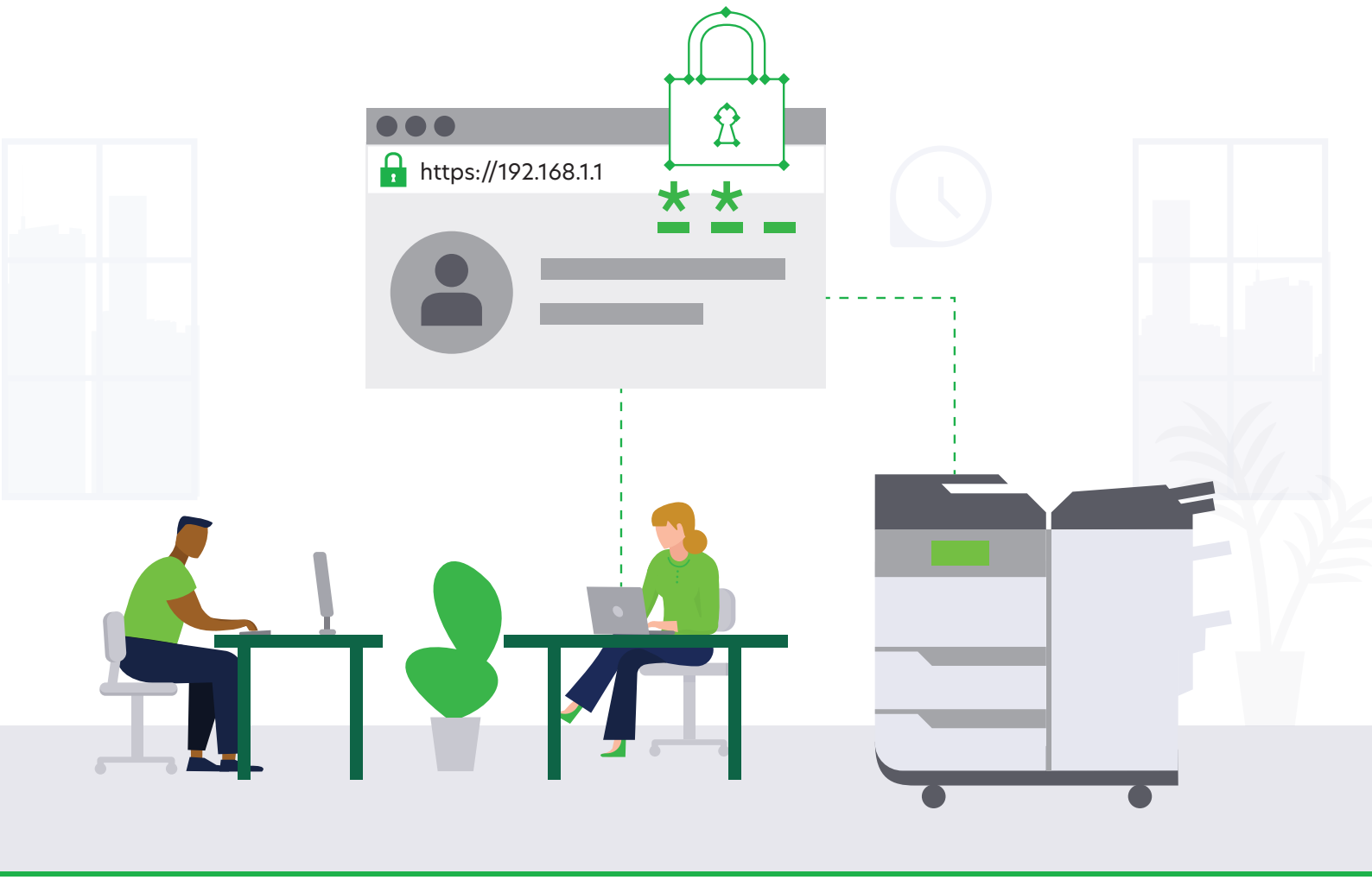
- **Separación de fax y red:** Lexmark ofrece una variedad de dispositivos multifunción que proporcionan funciones tanto de conectividad de red como de módem de fax. Para evitar cualquier interacción directa entre el módem y el adaptador de red, el hardware y el firmware del dispositivo Lexmark mantienen estos mecanismos separados.
- **Retención de fax entrante:** Los dispositivos Lexmark se pueden configurar para retener, en lugar de imprimir, los faxes entrantes durante las horas programadas. Los faxes entrantes se mantienen de forma segura en el disco duro hasta que en el dispositivo se introduzcan las credenciales correctas.




# Gestión remota segura

Para gestionar de manera eficiente un parque de impresoras en red, los dispositivos Lexmark incluyen funciones de seguridad que permiten que únicamente el personal autorizado configure el acceso a la red del dispositivo.

- **Acceso al dispositivo y a la configuración:** Los dispositivos Lexmark incluyen una variedad de controles de acceso a funciones, mecanismos de autenticación y autorización, y una contraseña de respaldo opcional para evitar que usuarios no autorizados modifiquen la configuración del dispositivo, incluida la configuración de seguridad.
- **Registro de auditoría con syslog seguro:** Permite realizar un seguimiento de los eventos relacionados con la seguridad para reducir riesgos, identificar posibles amenazas de forma proactiva e integrarlos con su sistema de detección de intrusiones para un seguimiento en tiempo real.
- **Flexibilidad de autenticación y autorización:** Los dispositivos Lexmark se pueden configurar para validar las credenciales de los usuarios y restringir las funciones del dispositivo mediante Active Directory y otras plataformas de servidores de directorio, incluyendo cuentas internas, Kerberos 5, LDAP, LDAP+GSSAPI, contraseña y PIN.
- **Seguridad de usuarios y grupos:** Esta función permite a los administradores conceder a usuarios individuales y a grupos de usuarios el derecho a acceder a funciones específicas del dispositivo, al mismo tiempo que restringe el acceso a otros usuarios o grupos.
- **Controles de acceso:** Los administradores pueden controlar el acceso local y remoto a determinados menús, funciones y flujos de trabajo en cada dispositivo. Losusuarios pueden desactivar completamente funciones como copiar, imprimir, enviar faxes, escanear a correo electrónico, FTP, trabajos retenidos, libreta de direcciones y más de 50 controles de acceso adicionales. El acceso a las funciones y menús del dispositivo se puede configurar seleccionando el permiso correspondiente para cada control de acceso.
- **Inserción automática de la dirección de correo electrónico del remitente:** Cuando un usuario se autentica para digitalizar un documento y enviarlo por correo electrónico, la dirección de correo electrónico del remitente se busca automáticamente y se inserta en el campo “De“. Esto permite que el destinatario vea claramente que el correo electrónico fue generado por esa persona y no de forma anónima ni desde el equipo multifunción.
- **Restricciones de inicio de sesión:** Los administradores pueden evitar el uso no autorizado de un dispositivo restringiendo el número de intentos de inicio de sesión fallidos consecutivos y registrando estos eventos mediante la auditoría integrada.




- **Gestión de certificados:** Las impresoras y los equipos multifunción de Lexmark pueden integrarse en un entorno PKI utilizando certificados firmados para autenticaciones HTTPS, TLS, IPsec y 802.1x.
- **HTTPS:** Los productos Lexmark pueden utilizar el protocolo HTTPS para cifrar el tráfico web, permitiendo que los usuarios realicen de forma segura la gestión remota a través de la página web integrada.
- **SNMPv3:** Las impresoras y los equipos multifunción de Lexmark admiten SNMPv3, incluidos los componentes de autenticación y cifrado de datos, lo que permite una gestión remota segura de los dispositivos. SNMPv1 y SNMPv2 también son compatibles y pueden configurarse o desactivarse de forma independiente.
- **Puertos USB protegidos:** Los puertos USB del host están diseñados teniendo en cuenta la seguridad y cuentan con varios mecanismos, incluida la posibilidad de desactivar los puertos e impedir que se utilicen de forma malintencionada.



# Estándares



Garantizar el cumplimiento
de certificaciones de terceros



# Estándares de seguridad

Como parte de nuestro enfoque integral en seguridad, Lexmark obtiene certificaciones conforme a estándares industriales y gubernamentales completos, y estas capacidades han sido validadas y certificadas por organizaciones externas reconocidas.

- **Certificación ISO 20243 de la cadena de suministro:** En cada paso de la cadena de suministro, Lexmark trabaja arduamente para garantizar que nuestros empleados, fabricantes y proveedores se atengan a los más altos estándares de cumplimiento, seguridad y responsabilidad social. Esto garantiza que los productos y las piezas que salen de producción se fabriquen exactamente según las especificaciones, lo que ofrece un producto auténtico y elimina los riesgos para su organización. De hecho, Lexmark es el primer proveedor de impresión en obtener la certificación de seguridad de la cadena de suministro ISO 20243 para todo el dispositivo de impresión, incluidos los cartuchos, los consumibles y las soluciones integradas.
- **Criterios Comunes (ISO/IEC 15408):** Los Criterios Comunes (Certificación NIAP/CCEVS, ISO 15408) representan un marco que facilita una validación de la funcionalidad de seguridad de un sistema informático. Dicha validación de terceros garantiza a los clientes que las funciones de seguridad protegen el dispositivo de la forma indicada por el fabricante. Los dispositivos se validan para la seguridad de dispositivos y sistemas de impresión en tecnología de la información, utilizando el perfil de protección vigente asociado al Esquema de evaluación y validación de Criterios Comunes (CCEVS).
- **FIPS 140-3 para la validación criptográfica:** NIST basa los requisitos y los estándares de los módulos criptográficos en FIPS. Lexmark utiliza un módulo OpenSSL validado según FIPS 140-3. FIPS 140-3 (que sustituye a FIPS 140-2) valida la seguridad, fiabilidad e integridad de los módulos criptográficos.
- **Perspectiva de analistas externos:** Desde el punto de vista de los analistas, el nivel de seguridad de los productos Lexmark ha sido reconocido por IDC, Quocirca y otros. Este reconocimiento, junto con nuestra cartera de certificaciones, ayuda a garantizar que los activos y datos de su organización estén protegidos.



# Gobernanza de seguridad

El equipo de Gobernanza de seguridad de Lexmark es responsable de garantizar las medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos. El enfoque integral de Lexmark en materia de seguridad ayuda a nuestros clientes a proteger la información sensible, al ofrecer productos y servicios altamente seguros en todos los sectores.

- **SOC 2 Tipo II para Lexmark Cloud:** Los servicios de nube de Lexmark han obtenido y mantienen la conformidad con el Control de la organización de servicios (SOC). Previa solicitud, el último informe SOC 2 tipo II está a disposición de clientes y potenciales clientes que tengan un acuerdo de no divulgación (NDA) activo. Desarrollado por el Instituto Americano de Contadores Públicos (AICPA), el SOC 2 define criterios para gestionar los datos de los clientes basados en cinco "principios de servicios de confianza": la seguridad, la disponibilidad, la integridad del procesamiento, la confidencialidad y la privacidad.
- **Gestión de la información según la ISO 27001:** Lexmark ha obtenido la certificación ISO 27001 por sus servicios de impresión administrada, servicios predictivos y servicios de configuración en la nube a nivel mundial. La ISO 27001 es un estándar internacional de sistemas de gestión de la seguridad de la información (SGSI) que proporciona un conjunto integral de requisitos para mantener la confidencialidad, integridad y disponibilidad de los datos.
- **Implementación de la estrategia de confianza cero:** El concepto principal del modelo de seguridad de confianza cero es "nunca confíe, siempre verifique", lo que significa que los usuarios y dispositivos no deben considerarse confiables por defecto, incluso si están conectados a una red autorizada. Lexmark comprende que las organizaciones están considerando los principios de confianza cero para aplicar controles de acceso más estrictos, tanto dentro como fuera del perímetro de la red. Teniendo esto en cuenta, asegurar un entorno empresarial se está volviendo cada vez más complejo y requiere un conocimiento integral del software, hardware, arquitectura de red y de los objetivos de seguridad de cada organización.
- **Programa de privacidad:** El programa de privacidad de Lexmark es una organización sólida compuesta por más de 80 empleados, tanto a nivel corporativo como en las unidades de negocio. La misión del programa es crear y mantener procesos repetibles diseñados para respetar y proteger la privacidad de los datos de nuestros clientes y sus usuarios, así como cumplir con las normativas de privacidad a nivel mundial.

Para obtener información más detallada, consulte el documento técnico de seguridad de Lexmark en https://www.xerox.es/oficina/latest/SECWP-06S.pdf

© 2026 Lexmark es una empresa de Xerox, registrada en Estados Unidos y/o en otros países. The Open Group Certification y Open Trusted Technology Provider son marcas comerciales y The Open Group es una marca comercial registrada de The Open Group. Para obtener más información sobre AICPA, visite www.aicpa.org/soc4so.
03/26 TSK-8685 SECGL-01SA