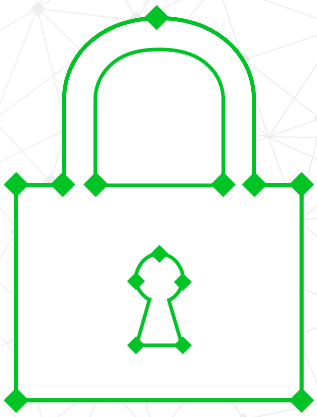
Guía de referencia de seguridad de Lexmark



Cuando se trata de seguridad, su organización debe garantizar que puede gestionar con eficiencia las impresoras en red, protegerlas contra los hackers y proteger la información más importante. En Lexmark, diseñamos nuestros dispositivos para satisfacer las necesidades de seguridad específicas de su empresa, con las funciones de seguridad más avanzadas de la industria.

Enfoque de Seguro por su diseño

La seguridad de un entorno empresarial es compleja y requiere conocimientos profundos del software, el hardware, la arquitectura de red, el contenido en la red, los factores humanos, y la posición y los objetivos de seguridad de cada organización. También requiere conocimiento experto para convertir conceptos de seguridad teóricos en productos y servicios seguros.

Lexmark no trata la seguridad como una característica opcional o de última hora, sino como un objetivo de diseño e ingeniería integral incluidos en todos nuestros productos y servicios. De hecho, este enfoque sistemático de seguro desde el diseño ofrece una ventaja decisiva a nuestros clientes: la confianza de dirigir su negocio de forma rentable, al saber que los dispositivos y los datos están protegidos en cada paso del proceso.

Nuestra comprensión de los entornos de red y las amenazas a la seguridad relevantes, especialmente en relación con la impresión, nos brinda el conocimiento práctico para crear soluciones exclusivas que protegen los datos en toda forma posible: una capacidad que hemos demostrado al trabajar y superar desafíos de seguridad en algunas de las organizaciones e industrias más reguladas del mundo.

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

Proteja todos los aspectos de la seguridad de impresión

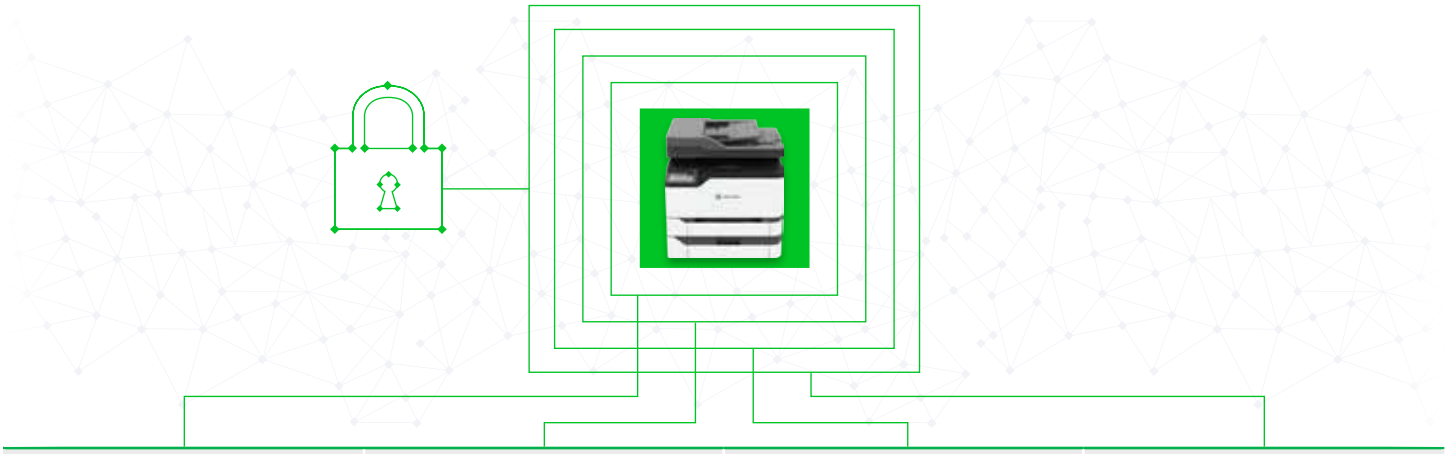
La experiencia de Lexmark como líder de la industria en seguridad de documentos y dispositivos forma la columna vertebral de nuestra tecnología. Nuestro perfil de seguridad para productos, soluciones, servicios y estándares, combinado con nuestro enfoque de Seguro por diseño, ayuda a los clientes a proteger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

Productos

Soluciones

Servicios

Estándares



Productos

- Verificación e inicio seguro del sistema operativo
- Módulo de plataforma segura
- Protección de memoria y almacenamiento
- Protección del firmware
- Separación de fax y red
- TLS 1.3
- Autenticación y autorización
- Acceso al dispositivo y a la configuración
- Seguro de forma predeterminada
- Borrado fuera de servicio
- Registros de auditoría con syslog seguro
- Gestión de certificados
- Puertos y protocolos seguros
- PrintCryption

Soluciones

- Cloud Print Management
- Cloud Fleet Management
- Análisis
- Lexmark Print Management
- Alianzas de software
- Secure Document Monitor
- Soluciones de tarjetas inteligentes
- Bandejas de papel bloqueables
- Markvision Enterprise
- Corrección automática
- Gestión automatizada de certificados
- Panel de seguridad

Servicios

- Evaluaciones de seguridad
- Gestión de la configuración
- Estrategia de gestión de seguridad
- Estrategia de actualización del firmware
- Gestión de vulnerabilidades

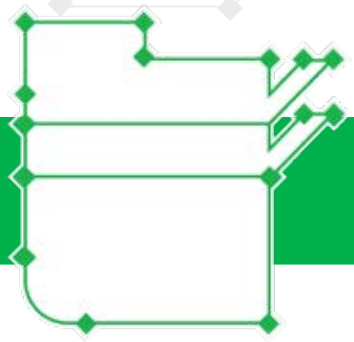
Estándares

- Criterios comunes (certificación NIAP/ CCEVS, ISO 15408)
- FIPS 140-2 (cifrado)
- SOC2 tipo II (nube)
- ISO 20243 (cadena de suministro)
- ISO 27001 (información)
- NIST (estándares)

Estos pilares son la base de un enfoque multifacético y de varias capas para garantizar el máximo nivel de seguridad de los dispositivos y datos en todo el proceso de impresión. Hemos integrado la seguridad en todos los dispositivos que producimos, desde las impresoras de escritorio más pequeñas hasta nuestros MFP empresariales más grandes, y todo lo demás. Esto significa que ya no tiene que elegir entre un dispositivo adecuado para su organización o uno que sea seguro.

Sin embargo, la seguridad de la impresión es solo una parte de la historia. Además de diseñar dispositivos resistentes a los riesgos, las soluciones avanzadas, los servicios de seguridad y las certificaciones de Lexmark trabajan conjuntamente para ofrecer una oferta de seguridad de salida completa que no tiene rival en la industria.

Productos

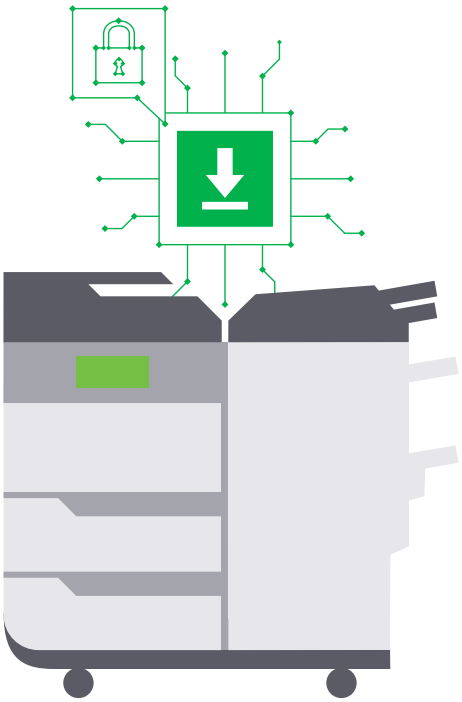


Mejore la seguridad de la impresora con el hardware y el firmware líderes del sector

Dispositivo protegido

Las impresoras y MFP de Lexmark ofrecen una oferta de seguridad sólida para la protección de los terminales y el refuerzo del sistema. Nuestras funciones de seguridad avanzadas permiten a los usuarios disminuir las amenazas y vulnerabilidades y a su vez mejorar su inversión en tecnología.

- **Tecnología de inicio seguro:** Los usuarios pueden validar que el firmware instalado en la impresora sea original de Lexmark. Si se detecta un firmware que no es original, el dispositivo mostrará una notificación de error.
- **Verificación continua:** Los administradores pueden asegurarse de que el firmware no haya sufrido alteraciones durante el funcionamiento. El código se vuelve a validar cada vez que se lee desde un almacenamiento persistente.
- **Firmware cifrado y firmado digitalmente:** Las impresoras y los MFP Lexmark inspeccionan automáticamente las actualizaciones de firmware descargadas para saber si cuentan con las firmas digitales respectivas de Lexmark. El firmware que no esté empaquetado correctamente ni firmado por Lexmark se rechaza.



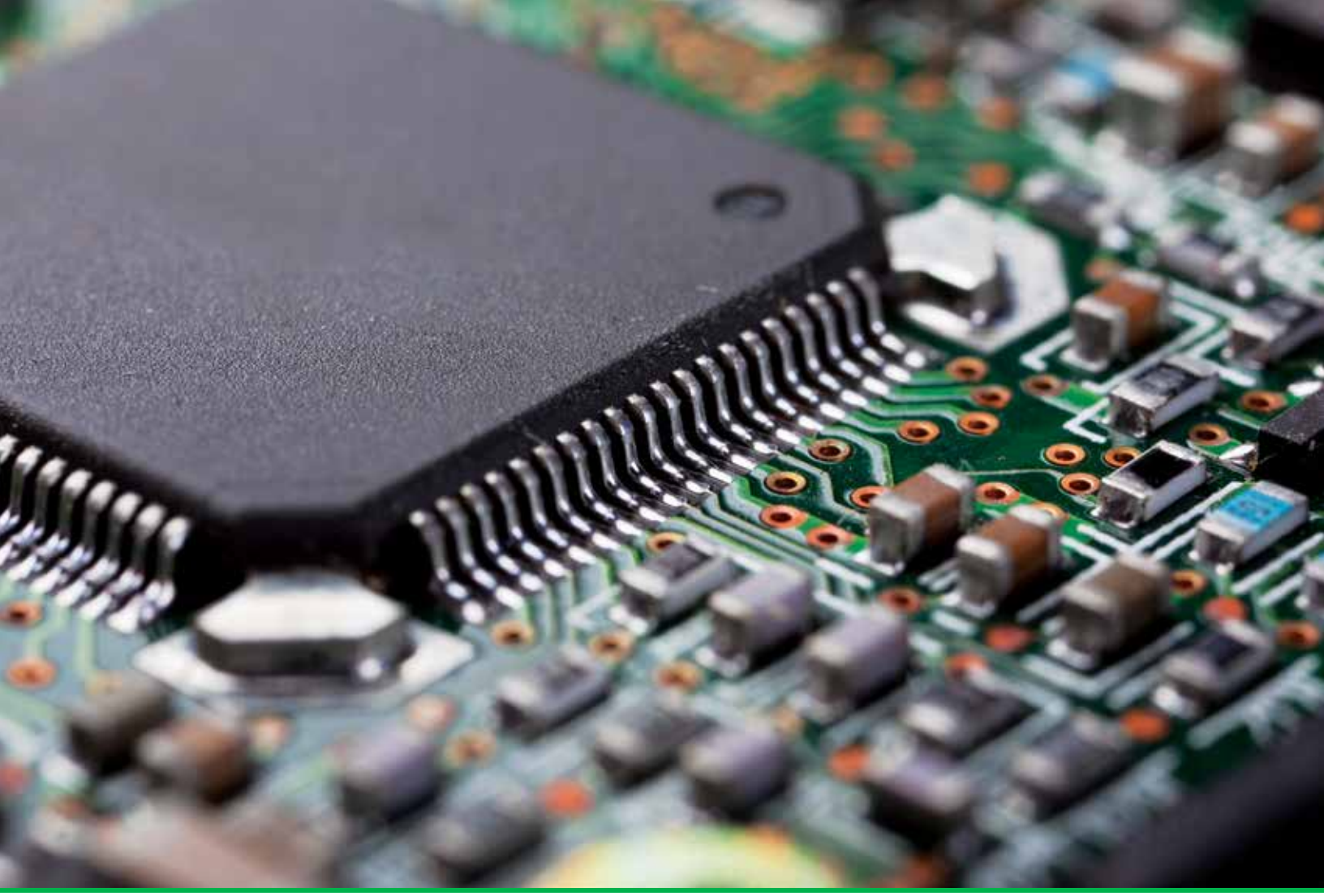
- **Integración con Active Directory:** Se proporciona compatibilidad con Microsoft Active Directory en los dispositivos Lexmark habilitados para la solución con pantallas táctiles. El uso de Active Directory para la última generación de dispositivos con pantalla táctil de Lexmark es un método seguro de autenticación y autorización que hace que la gestión de la seguridad de los dispositivos sea más rápida y sencilla para los recursos de TI.
- **Autenticación de tarjeta con y sin contacto:** Las soluciones de autenticación de credenciales incluyen soluciones de tarjetas con contacto y sin contacto para brindar autenticación básica. Esta opción se encuentra disponible cuando la identidad del usuario está vinculada a credenciales de identificación de seguridad de oficina. Las soluciones pueden verificar la identificación de la credencial y recuperar la información del usuario, de modo que el dispositivo Lexmark pueda acceder a trabajos de impresión retenidos, identificar el origen de documentos escaneados o identificar a un usuario para otros fines.

Todo el hardware, el software y el firmware de Lexmark se diseñan mediante los principios de seguridad que se describen en nuestro ciclo de vida de desarrollo de software seguro (SSDL, por sus siglas en inglés). El proceso aborda todos los aspectos de la seguridad, desde la planificación hasta el diseño y la implementación, e incluye el control de calidad, la liberación y el mantenimiento. También ofrece puntos de control de protección inigualables para cumplir con los estándares de seguridad más estrictos de su organización.

Datos seguros

Los dispositivos de Lexmark contienen una amplia gama de características diseñadas minuciosamente para mejorar la seguridad de los datos que se almacenan en el dispositivo y ayudar a impedir que usuarios maliciosos obtengan acceso a información confidencial.

- **Almacenamiento cifrado:** Hoy en día existen varias ubicaciones para almacenar datos en impresoras y en los MFP, que se pueden configurar para utilizar el cifrado. La impresora o el MFP genera internamente una clave AES de hasta 256 bits que se usa para cifrar todos los datos. La clave se almacena de forma no constante en el dispositivo, por lo que el contenido solo es accesible en la impresora o el MFP original. Los datos de un componente robado no serían accesibles aunque se instalara en un modelo idéntico de impresora o MFP.
- **Limpieza de archivos del disco duro:** Los datos que se escriban en discos duros de las impresoras o los MFP para el uso temporal al imprimir, escanear o fotocopiar se pueden borrar cuando se ha terminado el trabajo o después que se imprime un trabajo retenido para un usuario. Para garantizar que nunca se pueda recuperar la información, los discos duros de impresoras y dispositivos multifuncionales Lexmark eliminan la referencia del archivo en el directorio del disco y borran el archivo real en el disco, de modo que no se puedan leer datos residuales. Según el dispositivo, la limpieza del disco duro se puede configurar en modo manual, automático o programado. También se ofrece una limpieza en varias pasadas que cumple las normas del Instituto Nacional de Estándares y Tecnología (NIST) y del Departamento de Defensa (DOD).
- **Borrado completo del disco:** Antes de retirar, reciclar o quitar de un entorno seguro una impresora o un MFP, un usuario autorizado puede borrar completamente el disco. Esto incluye borrar los formularios, las fuentes, las macros o los trabajos retenidos no impresos que la limpieza de archivos del disco duro de rutina puede dejar atrás. Se ofrecen opciones de borrado de una o varias pasadas, lo que garantiza que no queden datos legibles en el disco.
- **Limpieza de memoria no volátil:** La limpieza de la memoria no volátil proporciona una herramienta para borrar todo el contenido almacenado en todas las formas de memoria flash que contiene el dispositivo. Esta característica es un borrado completo de todos los ajustes, soluciones, trabajos y faxes guardados en el dispositivo.
- **Borrado fuera de servicio:** Este proceso simplifica la eliminación de datos en todos los componentes de almacenamiento al quitar un dispositivo del servicio o eliminarlo de una ubicación segura. Los usuarios autorizados pueden realizar ambas acciones en un solo paso con el comando de limpieza “fuera de servicio”, disponible en el menú de configuración o en la página web del dispositivo.



- **Modo de plataforma segura:** A partir de nuestros anuncios de nuevos productos para 2022, ahora incluimos un módulo de plataforma segura (TPM, Trusted Platform Module) estándar que ofrece autenticación, comprobaciones de 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 a los usuarios al almacenar las claves de cifrado de la unidad de disco duro en una pieza de hardware distinta de los datos que cifra, con capas de protección añadidas. Este hardware también ayuda a reforzar el cifrado con una generación de números aleatoria mejorada.

Red segura

Desde la desactivación de características innecesarias hasta el bloqueo de interfaces de dispositivos y la protección de los datos que contienen, los dispositivos Lexmark incluyen un amplio rango de características integradas para fortalecer un dispositivo contra los ataques.

- **Filtro de conexión TCP:** Las impresoras y los MFP pueden configurarse para permitir conexiones TCP/IP únicamente desde una lista específica de direcciones TCP/IP para proteger el dispositivo de impresión y la configuración no autorizada.
- **Filtro de puerto:** Los puertos de red a través de los cuales las impresoras y los MFP escuchan o transmiten el tráfico de red son configurables, lo que permite tener un grado de control importante sobre la actividad de red del dispositivo. Los puertos de red y protocolos como telnet, FTP, SNMP, HTTP y otros se pueden desactivar explícitamente.
- **802.1x:** Con la autenticación del puerto 802.1x, las impresoras y los MFP pueden unirse a redes alámbricas e inalámbricas, al solicitar que los dispositivos se autentiquen antes de acceder a la red.
- **IPSec:** La opción de protocolo IPsec, cuando se activa, protege el tráfico de la red de dispositivos Lexmark con cifrado y autenticación. Esto protege los datos de impresión y el contenido de los trabajos escaneados en cualquier destino.
- **LDAP seguro:** A todo el tráfico LDAP desde y hacia dispositivos Lexmark se le puede otorgar seguridad con TLS. La información de LDAP como las credenciales, los nombres y las direcciones de correo electrónico que se intercambian mediante una conexión TLS se cifran para mantener la confidencialidad y la privacidad de los datos.

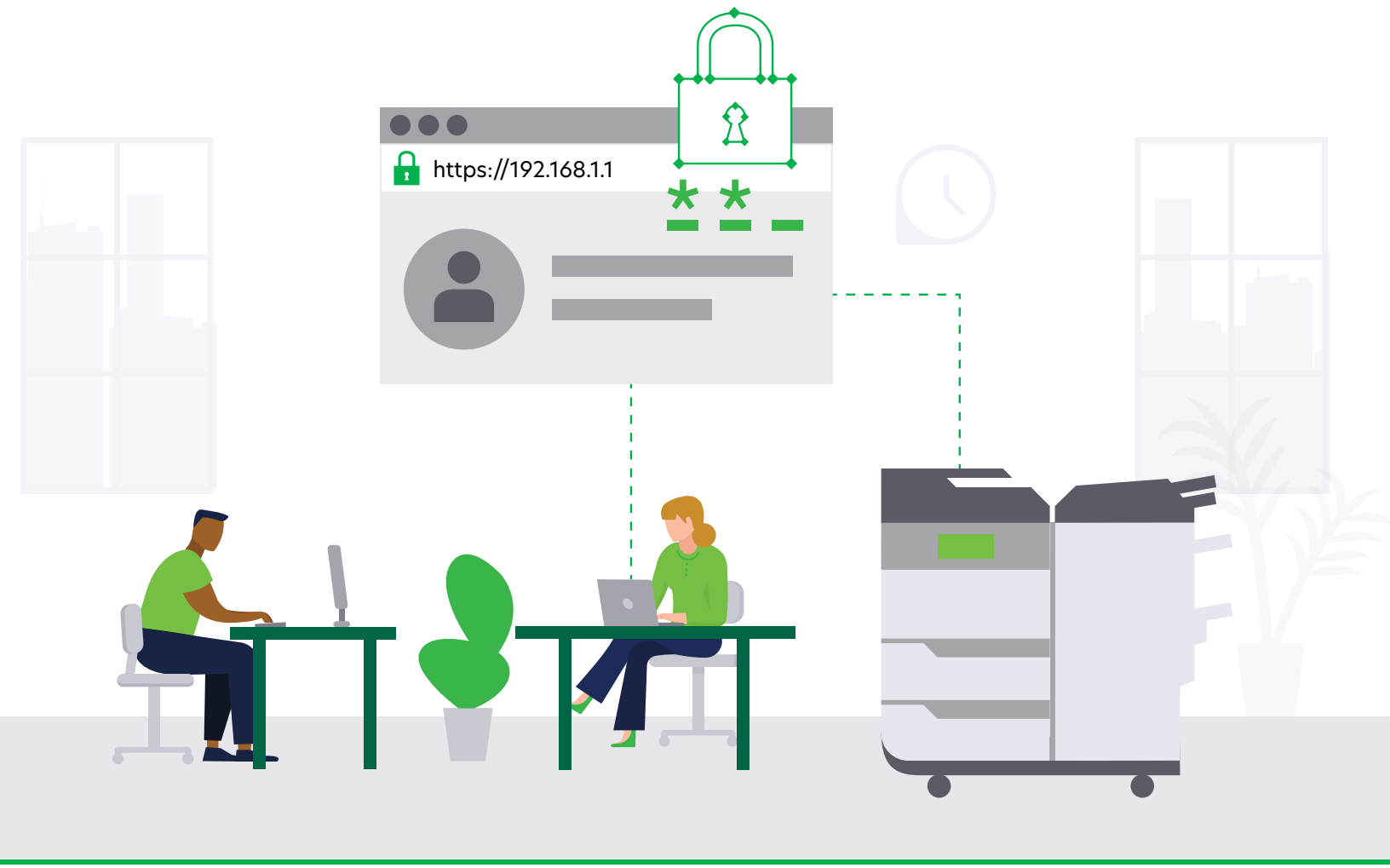
- **Seguro de forma predeterminada:** Seleccionar las opciones adecuadas para la configuración de seguridad de la impresora puede ser un gran reto. A partir del firmware 7, cuando los clientes optan por Seguro de forma predeterminada, existe la opción de crear una cuenta de administrador y el dispositivo apagará muchos puertos y protocolos antiguos que no son seguros y el cifrado del disco de inicio de forma predeterminada. Además, el asistente de configuración permite que su experiencia inicial sea sencilla y segura.

- **Separación de fax y red:** Lexmark ofrece una variedad de dispositivos MFP que proporcionan conectividad de red y de fax módem. Además, para impedir cualquier interacción directa entre el módem y el adaptador de red, el hardware y el firmware de los dispositivos Lexmark hacen que estos mecanismos funcionen de manera independiente.
- **Retención de faxes entrantes:** Los dispositivos Lexmark se pueden configurar para que retengan en lugar de que impriman los faxes entrantes durante horas programadas. Los faxes entrantes se retienen de manera segura en el disco duro hasta que se hayan ingresado las credenciales correctas en el dispositivo.

Administración remota segura

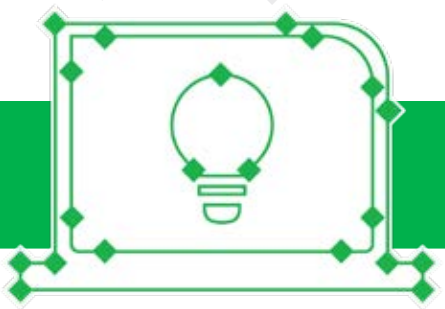
Para satisfacer las demandas de gestionar eficazmente una flota de impresoras en red, los dispositivos Lexmark disponen de las funciones de seguridad de gestión remota que necesita, ya que solo permiten al personal autorizado configurar el dispositivo para el acceso a la red.

- **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 impedir que usuarios no autorizados alteren la configuración del dispositivo, lo que incluye la configuración de seguridad.
- **Registro de auditorías con syslog seguro:** Haga un seguimiento de los eventos relacionados con la seguridad para reducir la exposición, rastree e identifique de manera proactiva los posibles riesgos e intégrelos en su sistema de detección de intrusos para lograr un seguimiento proactivo en tiempo real.
- **Flexibilidad de autenticación y autorización:** Los dispositivos Lexmark se pueden configurar para validar las credenciales del usuario y restringir las funciones de los dispositivos con Active Directory y otras plataformas de servidores de directorios, lo que incluye las cuentas internas, Kerberos 5, LDAP, LDAP+GSSAPI, la contraseña y el PIN.
- **Seguridad de usuarios y grupos:** Esta función permite a los administradores otorgarles a los usuarios individuales y los grupos de usuarios el derecho a acceder a funciones específicas del dispositivo, a la vez que restringe a otros usuarios o grupos.
- **Controles de acceso:.** Los administradores pueden controlar el acceso local y remoto a menús, funciones y flujos de trabajo específicos en cada dispositivo. Los usuarios pueden desactivar por completo funciones como copiar, imprimir, enviar por fax, escanear para enviar por correo electrónico, FTP, trabajos retenidos, libreta de direcciones y más de 50 otros controles de acceso. El acceso a las funciones y menús del dispositivo se puede establecer mediante la selección de un permiso para el respectivo 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, automáticamente se busca la dirección de correo electrónico del remitente y se inserta en el campo “De”. Esto permite al destinatario ver claramente que el correo electrónico lo generó esa persona y no es anónimo ni se envió desde el dispositivo multifuncional.
- **Restricciones de inicio de sesión:** Los administradores pueden impedir el uso no autorizado de un dispositivo al restringir el número de inicios de sesión fallidos consecutivos y realizar un seguimiento de estos eventos mediante la auditoría integrada.



- **Administración de certificados:** Las impresoras y los MFP Lexmark pueden integrarse en un entorno de PKI mediante certificados firmados para autenticaciones HTTPS, TLS, IPsec y 802.1x.
- **HTTPS:** Los productos de Lexmark pueden usar el protocolo de comunicación HTTPS para permitir que se cifre el tráfico web, de modo que los usuarios puedan llevar a cabo una gestión remota de forma segura a través de la página web integrada.
- **SNMPv3:** Las impresoras y los dispositivos multifuncionales Lexmark admiten SNMPv3, además de los componentes de autenticación y cifrado de datos, para permitir la gestión remota segura de los dispositivos. SNMPv1 y SNMPv2 también se admiten, y se pueden configurar o desactivar de manera independiente.
- **Puertos USB protegidos:** Los puertos host USB se diseñaron pensando en la seguridad, y cuentan con diversos mecanismos, entre los que se incluyen la capacidad de deshabilitar puertos y evitar que se utilicen de forma malintencionada.

Soluciones



Proteja los datos más valiosos
en todos los rincones de la red

Secure Fleet Management

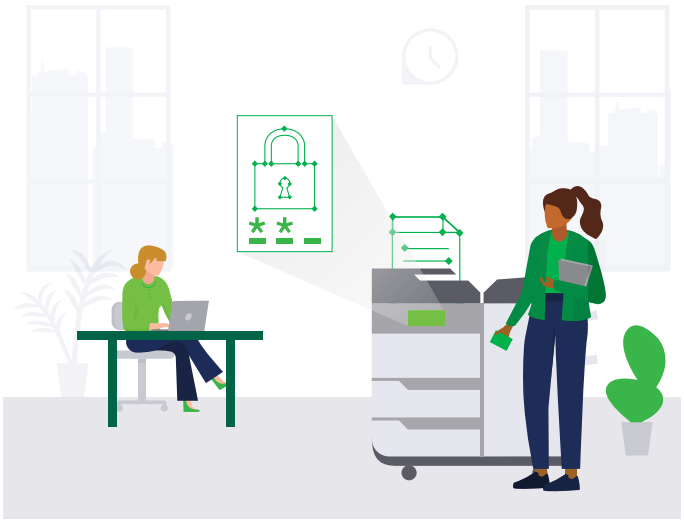
Las soluciones de gestión de seguridad de Lexmark son una parte fundamental del ecosistema de seguridad, lo que permite a los administradores gestionar flotas fácilmente y a la vez garantizar que los dispositivos cumplan con la postura de seguridad de nuestro cliente.

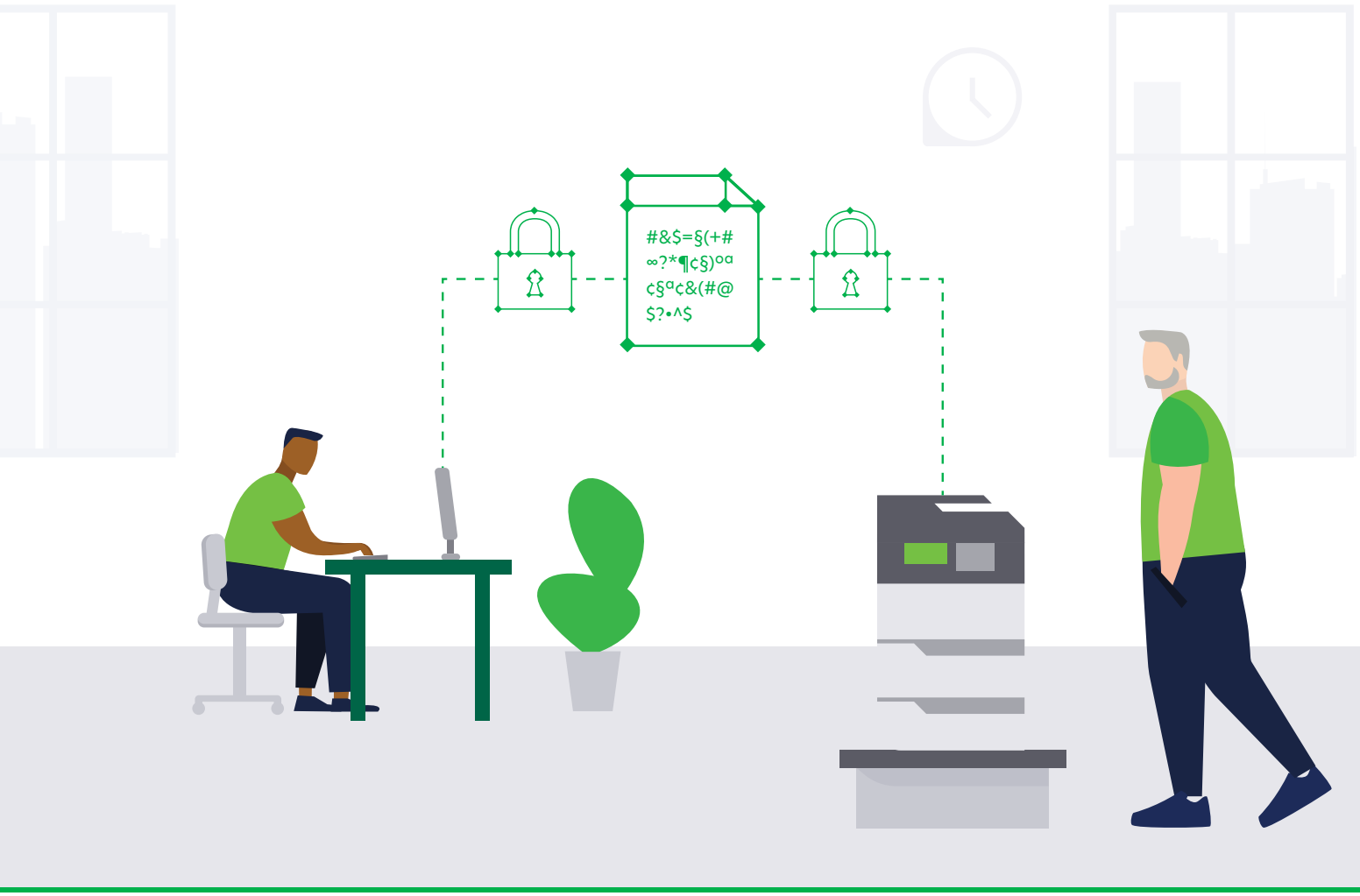
- **Lexmark Cloud Fleet Management (CFM)** es una solución de gestión de dispositivos Lexmark basada en la nube que facilita la configuración de impresoras, recopila estadísticas fundamentales y mantiene los dispositivos actualizados con el firmware y las aplicaciones recomendadas más recientes. Con Lexmark CFM, tras una única configuración, los dispositivos Lexmark se pueden gestionar desde cualquier lugar del mundo sin necesidad de desplazarse ni de estar en la misma red local. Esto da como resultado un ecosistema de impresión más actualizado y seguro, que elimina los vacíos de seguridad incluso en aquellas áreas de difícil acceso como las oficinas en casa o las ubicaciones por satélite.
- **Markvision Enterprise (MVE):** Con el fin de mejorar aún más las políticas de seguridad de su organización, contar con un software sólido de administración de la impresión es fundamental. Markvision Enterprise es un componente clave del enfoque "Seguro por su diseño" de Lexmark, que se diseñó con el fin de garantizar una seguridad óptima para cada dispositivo de la red. MVE es una solución de gestión de impresión fácil de usar que facilita a los clientes la configuración de los dispositivos y la actualización de las políticas de seguridad. Buyers Lab otorgó a MVE 4.0 de Lexmark el premio Platinum Tested Solution Award y MVE obtuvo una calificación de categoría mundial por sus innovaciones con configuraciones comunes, gestión automatizada de certificados, panel de seguridad y ventanas de actualización de firmware. Entre las funciones adicionales se incluyen la configuración automática y la aplicación de políticas básicas en dispositivos recién descubiertos, así como la corrección automática de los valores del dispositivo y el firmware que se determina que están fuera de las políticas. Estas funciones ayudan a minimizar las tareas manuales de TI, todo ello sin costo para el cliente.

Soluciones de seguridad

Lexmark ofrece soluciones innovadoras de software y hardware que amplían las capacidades del dispositivo y ayudan a proteger los datos confidenciales de su organización.

- **Lexmark Cloud Print Management (CPM)** proporciona una impresión basada en la nube más rápida y segura con menos carga para los recursos de TI de la organización. En vez de enviar documentos a través de un servidor de impresión a un dispositivo de impresión designado donde las páginas permanecen a la vista del público hasta que se retiran, se transfieren a Lexmark Cloud donde quedan retenidos en una cola personal hasta que el usuario se autentica al ingresar su PIN o pasa su credencial por la impresora.
- **Lexmark Print Management (LPM):** Con Lexmark Print Management, los usuarios envían documentos desde su computadora, tableta o smartphone a cualquier impresora o producto multifuncional (MFP, por sus siglas en inglés) habilitado. En lugar de "enviar" los documentos a una impresora designada donde las páginas impresas permanecen a la vista del público hasta que alguien las retire, los usuarios de LPM deben "extraer" los archivos de la cola de impresión al iniciar sesión o pasar su tarjeta de identificación en la impresora.
- **Impresión confidencial:** Al retener los trabajos en una impresora o un MFP Lexmark específico hasta que se libera con un PIN, la impresión confidencial evita que los curiosos vean los documentos en la bandeja de impresión.





- **PrintCryption protege** la información confidencial, ya que el trabajo de impresión se cifra en la estación de trabajo del usuario y se descifra en el dispositivo de impresión de red. Este nivel de seguridad de impresión es ideal para las empresas que gestionan información empresarial privada altamente confidencial, relacionada al personal, financiera, médica, y técnica. PrintCryption también permite un mejor cumplimiento de las normativas y admite varios niveles de cifrado AES.
- **Bandejas de papel bloqueables:** Varios modelos de Lexmark admiten una bandeja bloqueable opcional que se puede utilizar para proteger el papel confidencial y reducir el riesgo de robo de papel.
- **Lexmark Secure Document Monitor** reside en los MFP de Lexmark de una organización para capturar de forma automática y discreta el contenido y los datos de usuario de todos los documentos que pasan. Esto permite la captura en tiempo real, sin interrumpir ni retrasar los procesos ni el rendimiento. A partir de ahí, los datos capturados se envían sin problemas al sistema DLP o de supervisión de la organización. Si un cliente busca una opción más sólida que proporcione supervisión y protección de extremo a extremo, Lexmark ofrece una solución combinada que está formada por LSDM con innerActiv.

- **Compatibilidad con tokens CAC/PIV/SIPR del gobierno de EE. UU.:** Lexmark colabora con 90Meter para aprovechar las ventajas de la seguridad de las tarjetas inteligentes. La tarjeta de acceso común (CAC, por sus siglas en inglés) y la solución de autenticación de verificación de identidad personal (PIV, por sus siglas en inglés) les proporciona a los procesos de flujo de trabajo seguros un mayor control de la seguridad de los MFP de Lexmark en red en operaciones del gobierno federal. La solución también admite tokens SIPR para proporcionar acceso a través de la red secreta de enrutadores de protocolo de internet.

- **Compatibilidad con la autenticación de tarjetas inteligentes:** Lexmark es compatible con varios tipos de tecnologías de tarjetas inteligentes para garantizar la seguridad de los documentos y los datos confidenciales.

- **Las alianzas de software** ofrecen a los clientes una oportunidad única para aprovechar las mejores soluciones de nuestros socios de software a fin de implementar una cartera de tecnología completa, todo desde una única fuente. Mejoramos y aumentamos nuestras protecciones en seguridad de la impresión mediante colaboraciones bien estudiadas. Esto nos permite ayudar a los clientes de todo el mundo a crear un estado ideal para abordar necesidades de seguridad muy específicas tanto en los departamentos como en la organización. Lexmark tiene relaciones con socios formales como Elatec, HID Global, innerActiv, Upland, Kofax, Pharos, Ringdale, Papercut, LRS, Retarus, Plus Tech, etherFax y muchos más.

Servicios

Simplifique la gestión de la impresión a la vez que aumenta la seguridad

Estrategias de seguridad

Lexmark responde a las amenazas de datos con un enfoque sistemático que abarca el dispositivo, la flota y toda la infraestructura de red. Nuestra comprensión de los entornos de red y las amenazas de seguridad relevantes nos proporciona la experiencia necesaria para crear soluciones únicas que protejan sus datos de todas las maneras posibles.

- **Estrategia de gestión de seguridad:** Las ventajas de una estrategia de seguridad son numerosas y medibles. Una estrategia eficaz garantiza la confidencialidad, la integridad y la disponibilidad de la información, así como también proporciona protección para los dispositivos y los datos, tanto interna como externamente. Lexmark colabora estrechamente con los clientes para garantizar que las soluciones de seguridad estén alineadas con los requisitos específicos de su organización para ayudar a mitigar los riesgos y protegerse de la pérdida de ingresos.
- **Estrategia de actualización del firmware:** El desarrollo de una estrategia de actualización de firmware garantiza que una organización pueda aprovechar las últimas funciones del dispositivo, la velocidad y las mejoras de eficiencia. Si los dispositivos no se ejecutan en la última versión, el riesgo de filtraciones aumenta exponencialmente y puede poner en riesgo los datos confidenciales. Lexmark ayuda a los clientes a desarrollar una estrategia completa de actualización de firmware para aprovechar las últimas funciones del dispositivo, las correcciones rápidas y las correcciones de seguridad a fin de abordar las vulnerabilidades conocidas y ofrecer una protección óptima.
- **Gestión de vulnerabilidades:** En Lexmark, la reducción de la exposición a las vulnerabilidades es nuestra prioridad, de modo que los usuarios puedan concentrarse en apoyar a los clientes y proteger los activos fundamentales. Como lo define nuestro SSDL, los expertos en seguridad de Lexmark supervisan de forma constante varios canales para identificar posibles vulnerabilidades de seguridad. Si surge la necesidad, nuestros expertos reaccionan con rapidez para eliminar la exposición a la amenaza y divulgar de manera responsable la corrección.

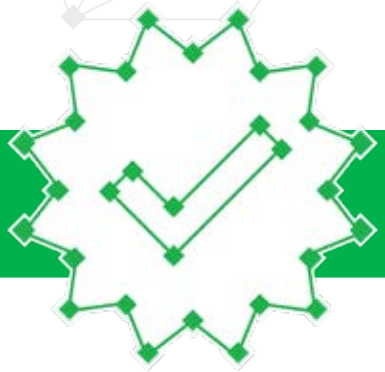
El enfoque de industria de Lexmark permite que nuestros dispositivos y soluciones prosperen en todos los ámbitos, entre los que se incluyen el gobierno, la sanidad, el comercio minorista, la banca, la industria manufacturera, la educación y muchos más. De hecho, contamos con asesores de la industria cuyo único objetivo se centra en los desafíos específicos a los que se enfrenta su industria, como los problemas de cumplimiento normativo, independientemente de su tamaño o ubicación en el mundo.

Servicios de seguridad

Lexmark proporciona seguridad de impresión de nivel superior al ofrecer dos soluciones dentro de los servicios de seguridad Managed Print Services (MPS): La evaluación de la seguridad permite identificar riesgos, vulnerabilidades y oportunidades de seguridad, mientras que la gestión de la configuración protege los ecosistemas de impresión y escaneo mediante la estandarización y la supervisión continua.

- **Evaluaciones de seguridad** Descubra las preocupaciones de seguridad de su flota de impresión y escaneo ahora y en el futuro con evaluaciones programadas con regularidad para detectar e informar sobre el estado de sus dispositivos Lexmark. Al aprovechar este conjunto de servicios, Lexmark ayudará a reducir los riesgos de seguridad de su flota y a crear un conjunto personalizado de recomendaciones proporcionadas por nuestros expertos en seguridad.
- **Gestión de la configuración:** Lexmark implementará las recomendaciones aprobadas por el cliente que se generaron durante la evaluación de seguridad. Con nuestro amplio conjunto de funciones de gestión de dispositivos basadas en la nube y en las instalaciones, los equipos de asistencia de Lexmark implementarán actualizaciones de firmware, supervisarán y aplicarán configuraciones de dispositivos seguras e informarán sobre los niveles y la actividad de conformidad.

Estándares



Garantice el cumplimiento con las certificaciones de terceros

Estándares de seguridad

Como parte de nuestro enfoque integral en materia de seguridad, Lexmark obtiene certificaciones de estándares integrales gubernamentales y de la industria, por lo que estas capacidades han sido validadas y certificadas por reconocidas organizaciones de terceros.

- **Certificación ISO 20243 de la cadena de suministro:** En cada etapa de la cadena de suministro, Lexmark trabaja incansablemente para garantizar que nuestros empleados, fabricantes y proveedores cumplan los estándares más exigentes de cumplimiento normativo, con la seguridad y la responsabilidad social. De esta forma, se garantiza que los productos y las piezas que se producen se hayan creado tal y como se especifica. Así, se obtiene un producto auténtico y se eliminan los riesgos para su organización. De hecho, Lexmark es el primer proveedor de impresión con una certificación ISO 20243 de seguridad de la cadena de suministro para todo el dispositivo de impresión, incluidos los cartuchos, los insumos y las soluciones integradas.
- **Criterios comunes ISO/1EC 15408:** Common Criteria (certificación NIAP/CCEVS, ISO 15408) proporciona una estructura para validar la funcionalidad de la seguridad de un sistema computacional. Tal proceso de validación de terceros confirma a los clientes que las capacidades de seguridad protegen al dispositivo como lo indica el fabricante. Los dispositivos se validan para Information Technology Hardcopy Device and System Security con el perfil de protección actual asociado al esquema de evaluación y validación de criterios comunes (CCEVS, por sus siglas en inglés).
- **FIPS 140–2 para la validación de la criptografía:** El NIST basa los requisitos y los estándares de los módulos criptográficos en los estándares FIPS. Lexmark ha completado un programa de validación de algoritmos criptográficos (CAVP, por sus siglas en inglés) 140-2 de FIPS en productos Lexmark, una validación independiente de la implementación correcta de algoritmos criptográficos que se usan en nuestros dispositivos.
- **Perspectiva de los analistas de terceros:** Desde la perspectiva de un analista, la postura de seguridad de los productos Lexmark fue reconocida por IDC, Quocirca y otros. Este reconocimiento y nuestra cartera de certificaciones contribuyen a garantizar la protección de los activos y los datos de su organización.

Regulación de la seguridad

El equipo de Regulación de la seguridad de Lexmark es responsable de asegurar las garantías para proteger la confidencialidad, la integridad y la disponibilidad de los datos. El enfoque integral de Lexmark en materia de seguridad ayuda a nuestros clientes a proteger la información confidencial al ofrecer productos y servicios de alta seguridad en todas las industrias.

- **SOC 2 tipo II para Lexmark Cloud:** Lexmark Cloud Services ha logrado y mantiene el cumplimiento de control de la organización de servicios (SOC, por sus siglas en inglés). El último informe SOC 2 tipo II está disponible mediante solicitud para los clientes y posibles clientes que tienen un acuerdo de no divulgación (NDA) activo. Desarrollado por el American Institute of CPAs (AICPA), SOC 2 define criterios para gestionar los datos de los clientes según los cinco "principios de servicios de confianza": la seguridad, la disponibilidad, la integridad de procesamiento, la confidencialidad y la privacidad.
- **Gestión de la información ISO 27001:** Lexmark obtuvo la certificación ISO 27001 para sus Managed Print Services, servicios predictivos y servicios de configuración en la nube en todo el mundo. El ISO 27001 es un estándar internacional del sistema de gestión de seguridad de la información (ISMS) que proporciona un conjunto completo de requisitos para mantener la confidencialidad, la integridad y la disponibilidad de los datos.
- **Implementación de la estrategia confianza cero:** El principal concepto detrás del modelo de seguridad de confianza cero es "nunca confíe, siempre verifique", lo que significa que no se debe confiar de antemano en los usuarios y dispositivos, incluso si están conectados a una red con permiso. Lexmark comprende que las organizaciones están teniendo en cuenta los principios de confianza cero para proporcionar controles de acceso más estrictos, tanto dentro como fuera del perímetro de la red. Por ello, la seguridad de un entorno empresarial es cada vez más compleja y requiere un conocimiento exhaustivo del software, el hardware, la arquitectura de red y los objetivos de seguridad de cada organización.
- **Programa de privacidad:** El programa de privacidad de Lexmark es una sólida organización de más de 80 empleados tanto a nivel corporativo como de unidades comerciales. La misión del programa es la creación y el mantenimiento de procesos repetibles diseñados para respetar y proteger la privacidad de los datos de nuestros clientes y de sus usuarios, así como también para cumplir las normativas de privacidad mundiales.

Para obtener información más detallada, consulte el informe técnico de seguridad de Lexmark en https://www.lexmark.com/securitywhitepaper