

# Capas

Cómo crear una estrategia de seguridad efectiva para asegurarse de que la impresión no sea su eslabón débil.



# La seguridad de impresión multicapa es más eficaz

Según la firma de análisis de tecnología Quocirca, el 61% de las organizaciones han experimentado pérdida de datos en el último año debido a prácticas de impresión no seguras.<sup>1</sup> La seguridad es más que la funcionalidad del dispositivo y necesita funcionar en múltiples niveles. Una estrategia de múltiples capas que funcione a nivel de hardware, software y red es el enfoque más efectivo y se explora a continuación.

- 1 Un enfoque contundente
- 2 El software seguro importa
- 3 Apoyo a la seguridad de la red
- 4 La diferencia de Lexmark

<sup>1</sup>Quocirca Print Security Landscape 2023

## Acerca de Lexmark

Lexmark ofrece una seguridad de impresión sin igual, con nuestras soluciones que se encuentran en algunos de los entornos más regulados y conscientes de la seguridad del mundo, incluidas las agencias federales y los servicios financieros. Desde dispositivos diseñados de forma segura y software de gestión remota hasta la gestión continua de vulnerabilidades y configuraciones, los productos, soluciones y servicios de Lexmark cuentan con la certificación independiente de los más altos estándares, incluidos los criterios comunes y los estándares federales de procesamiento de información (FIPS).



# Un enfoque contundente



Cómo el diseño y desarrollo de hardware afecta a la seguridad de impresión y qué buscar como parte de un enfoque de mejores prácticas.

Tres consideraciones clave:

## Seguro por diseño

Sus impresoras y MFP deben tener la seguridad integrada como un objetivo integral de diseño e ingeniería, no solo como una característica opcional / adicional. Este enfoque de ingeniería segura crea salvaguardas en el dispositivo físico como estándar para mejorar la seguridad de los datos y ayuda a evitar que usuarios malintencionados accedan a información confidencial. También es compatible con su estrategia de seguridad de puntos finales.

## Firmware cifrado y firmado digitalmente

El firmware del dispositivo contribuye directamente a la seguridad del dispositivo. Busque configuraciones "listas para usar" que, una vez promulgadas, no pueden ser alteradas por usuarios no autorizados. Las protecciones de firmware, memoria, almacenamiento y sistema operativo seguro incluyen almacenamiento cifrado, limpieza de archivos del disco duro, tecnología de arranque seguro, verificación continua y más. Estas características no solo ofrecen una protección óptima, sino que reducen las tareas manuales y alivian la carga de los recursos de TI.

## Verificado de forma independiente según los estándares de terceros

Cualquiera puede decir que sus dispositivos son seguros. Asegúrese de que sus impresores (y más ampliamente, sus soluciones de impresión) estén certificados según los estándares internacionales y de la industria relevantes,

**Los analistas dicen: 'Los dispositivos Lexmark admiten una gama completa de funciones integradas para el endurecimiento de dispositivos y la protección de puntos finales.'**

IDC MarketScape: Soluciones y servicios de seguridad en todo el mundo 2022-2023



como Common Criteria y FIPS. La integridad de la cadena de suministro afecta a la seguridad. La certificación ISO 20243 extiende esta regulación a toda la cadena de suministro para darle la confianza de que sus dispositivos realmente son a prueba de manipulaciones y nunca falsificados.

Lexmark es el primer proveedor de soluciones de impresión en recibir la certificación ISO 20243 para la integridad de la cadena de suministro, abordando la seguridad desde el desarrollo del producto hasta la fabricación y distribución.

## Para llevar

- Los dispositivos de impresión deben tener protección de seguridad integrada.
- El firmware debe estar encriptado y firmado digitalmente.
- Verifique que se cumplan plenamente los estándares independientes de la industria.



# El software seguro importa



Cómo las soluciones de impresión basadas en software pueden mejorar la seguridad tanto del dispositivo como de su entorno operativo.

Tres consideraciones clave:

## Ciclo de vida de desarrollo de software seguro (SSDL)

El software utilizado para soportar impresoras puede ser un punto débil para la seguridad. Busque un proveedor que tenga un SSDL para mitigar esto y optimizar la protección. ¿Cómo? Al abordar de manera integral todos los aspectos de la seguridad relacionados con el desarrollo de software, desde la planificación hasta el diseño y la implementación. Esto significa, por ejemplo, que antes de enviar cualquier código, se somete a pruebas multipunto para verificar si hay vulnerabilidades y estabilidad del código.

## Capacidad de gestión remota

Los cambios en los patrones de trabajo (como trabajar desde casa y entornos de trabajo híbridos) se suman a la complejidad de administrar de forma segura una flota de dispositivos de impresión en red, además de abrir el potencial de vulnerabilidades. En esta nueva realidad, el software de impresión robusto para la gestión remota es una necesidad. Las características como la configuración común, la administración automática de certificados y las actualizaciones de firmware en tiempo especificado garantizan que el cumplimiento de la seguridad esté completamente actualizado en toda la empresa. También se impide que el personal no autorizado altere cualquier configuración del dispositivo.

## Aplicaciones de usuario relacionadas con la seguridad.

La funcionalidad basada en software, como la liberación de impresión segura, puede mejorar la protección y la confidencialidad de los datos. Este tipo de aplicación restringe

'Un SSDL aborda todos los aspectos de la seguridad de impresión para ofrecer puntos de control de protección sin precedentes.'

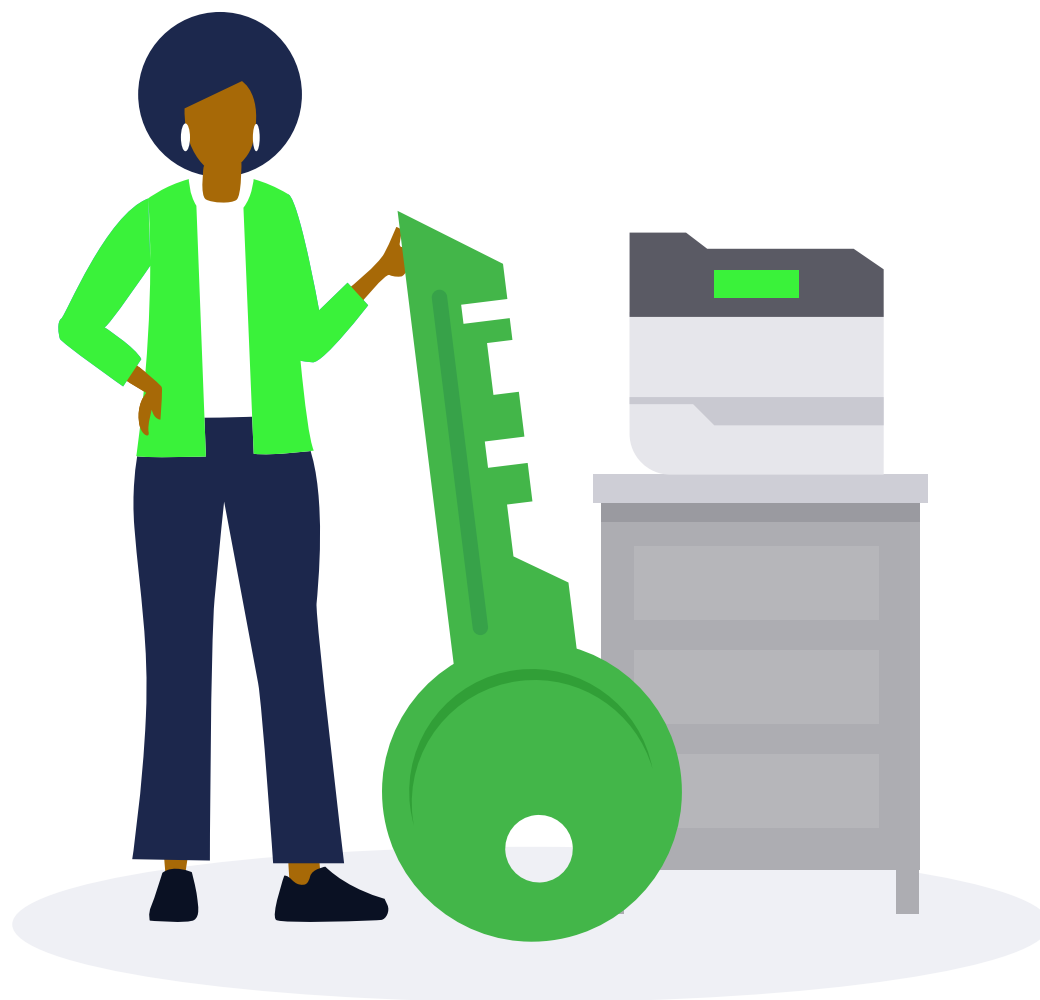


el acceso al tiempo que brinda a los usuarios la flexibilidad de imprimir desde cualquier lugar. Se opera a través de ID de usuario de red segura y puede ser a través de autenticación sin contacto o con tarjeta inteligente. Ciertos sectores, como las operaciones del gobierno federal, requieren una mayor seguridad de los documentos. Para estas industrias, busque soluciones que admitan entornos de administración de certificados automatizados y soluciones de autenticación de tarjetas de acceso comunes (CAC) y verificación de identificación personal (PIV).

Garantice el cumplimiento de la seguridad en toda su organización con Lexmark Markvision Enterprise. Este software de gestión de impresión gestiona tanto la configuración del dispositivo como las políticas de seguridad en una única herramienta fácil de usar.

## Para llevar

- Un SSDL mejora la seguridad de impresión.
- El software de gestión remota es imprescindible.
- Busque funciones de impresión segura basadas en software.



# Apoyo a la seguridad de la red



Cómo garantizar que su infraestructura de impresión en red ayude a proteger una integridad de red más amplia.

Tres consideraciones clave:

## Identificación y gestión de vulnerabilidades

Su entorno de red y las amenazas de seguridad relevantes son únicas, lo que significa que necesita una solución personalizada para proteger sus datos. La evaluación de las brechas de seguridad es clave para desarrollar una infraestructura de impresión que proteja adecuadamente los puntos finales y los puntos de entrada de los dispositivos de los usuarios finales. La capacidad de modelado de amenazas de su proveedor de impresión también puede ayudar a analizar y reducir el potencial de ataques.

## Monitorización continua de la configuración

Reducir la exposición a vulnerabilidades en toda la red es fundamental. La supervisión continua de la configuración, el firmware y las vulnerabilidades potenciales reduce significativamente el perfil de riesgo de la impresión y simplifica las actualizaciones y los ajustes de configuración necesarios para mantener la seguridad.

## Análisis de datos de rendimiento en tiempo real

Las soluciones de impresión basadas en la nube respaldan la mejora de la seguridad de los puntos finales a través de la captura y el análisis de datos, lo que facilita la identificación de anomalías y la alerta sobre patrones de uso sospechosos y posibles violaciones de seguridad. La visibilidad en todo el sistema mejora el control al tiempo que reduce el riesgo de seguridad, y es particularmente importante para industrias altamente reguladas como la salud, el gobierno y los servicios financieros.

**'Lexmark también debe estar en la lista corta de proveedores al considerar factores como la seguridad para enfrentar los desafíos del trabajo híbrido, mover la infraestructura de impresión a la nube, desarrollar una postura de seguridad sólida que pueda expandirse y evolucionar con el tiempo, y la necesidad de una prestación de servicios global consistente.'**

IDC MarketScape: Evaluación de proveedores de soluciones y servicios de seguridad en todo el mundo 2022-2023



Los servicios de seguridad de Lexmark incluyen evaluaciones de seguridad, optimización de la configuración y gestión de vulnerabilidades para crear un ecosistema de impresión seguro incluso para los desafíos de protección de datos más complejos.

## Para llevar

- Asegúrese de que sus soluciones de impresión son compatibles con la protección de puntos finales.
- La configuración debe alinearse con la seguridad de la red.
- El análisis de datos identifica el uso sospechoso en tiempo real.





# La diferencia de Lexmark

## Seguro por diseño: protección en todos los niveles

El exclusivo enfoque Secure by Design de Lexmark incorpora la seguridad en todos nuestros productos, servicios y soluciones para mejorar su estrategia de protección de puntos finales. Secure by Design trata la seguridad como un objetivo integral de diseño e ingeniería en el diseño de productos, la integridad de la cadena de suministro, las funciones de seguridad avanzadas, la gestión de vulnerabilidades y las certificaciones de terceros para que sepa que los dispositivos y los datos están protegidos en cada paso del camino.

## Seguridad de impresión multicapa

Nuestro enfoque sistemático para imprimir la protección de capas de seguridad en dispositivos, datos e información para proporcionar un ecosistema seguro para su empresa que respalde una estrategia de confianza cero.

- 1 Productos: el hardware y el firmware líderes del sector mejoran la seguridad de la impresora.
- 2 Soluciones: proteja sus datos más valiosos en cada punto de la red.
- 3 Servicios: simplifique la gestión de impresión a la vez que mejora la seguridad.
- 4 Estándares: asegúrese de cumplir con las certificaciones de terceros.



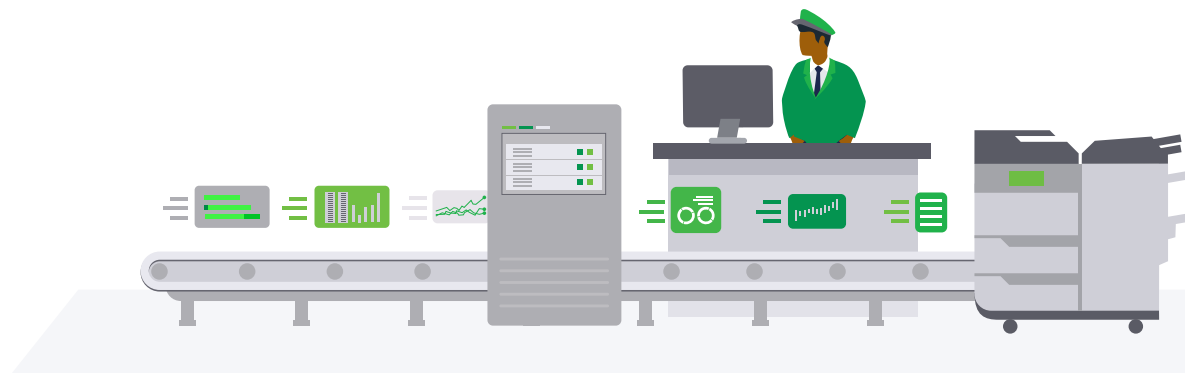
## Lexmark trabaja con...

7 de los 10  
principales  
bancos mundiales

7 de las 10  
principales  
agencias federales  
de EE. UU.

‘La seguridad básica está integrada  
en todos los productos de Lexmark.’

Panorama de seguridad de impresión de Quocirca, 2023



Más información en [Lexmark.com](https://www.lexmark.com)

Ponte en contacto

