Asegúrate que tu impresora y tu red estén protegidas

Comparación entre Ricoh y HP

Las impresoras y multifuncionales de hoy tienen las mismas vulnerabilidades que otros dispositivos en la red. Todas ellas contienen información y datos confidenciales que las convierten en los principales objetivos de una violación de seguridad.

Por ello, es fundamental tomar en cuenta la forma en la que tu tecnología de impresión aborda este tema para reducir el riesgo y proteger tus dispositivos, documentos, datos y negocios.

Ricoh asegura brindar una gran gama de seguridad para minimizar el riesgo y, dada la importancia de este tema en el trabajo, vale la pena comparar las medidas de seguridad de Ricoh con las de HP.

Medidas de seguridad de Ricoh

Ricoh destaca tres medidas de seguridad en sus impresoras:

- **Detección de intrusos:** Para Ricoh, una multifuncional puede identificar a los usuarios. Las funciones de autenticación de usuario de Ricoh se basan en códigos de hasta ocho dígitos o en combinaciones de nombres y contraseñas para el inicio de sesión. Asimismo, sus multifuncionales permiten la identificación del usuario a través de un sistema de autenticación existente.[1]
- **Detección de dispositivos:** Para evitar que el firmware original sea reemplazado por un firmware no autorizado, Ricoh utiliza firmas electrónicas con el fin de validarlo. Además, el Módulo de Plataforma Confiableo (TPM, por sus siglas en inglés), un hardware inviolable de módulo de seguridad, valida la autenticidad para el firmware de la multifuncional y las aplicaciones instaladas antes de permitir que la impresora funcione. Estas tecnologías garantizan la seguridad del dispositivo.
- **Protección de datos y documentos:** Para aumentar la seguridad contra el uso no autorizado, los archivos en formato PDF pueden protegerse mediante un cifrado y contraseña. Usando la función de bloqueo de la impresión, se asigna una contraseña al enviar el documento, la cual debe ser introducida en la multifuncional antes de imprimir. La función de copia de seguridad imprime / copia documentos con patrones invisibles puestos en el fondo. Las libretas de direcciones, la autenticación de la información y los documentos están cifrados de la forma en la que están almacenados en la multifuncional.

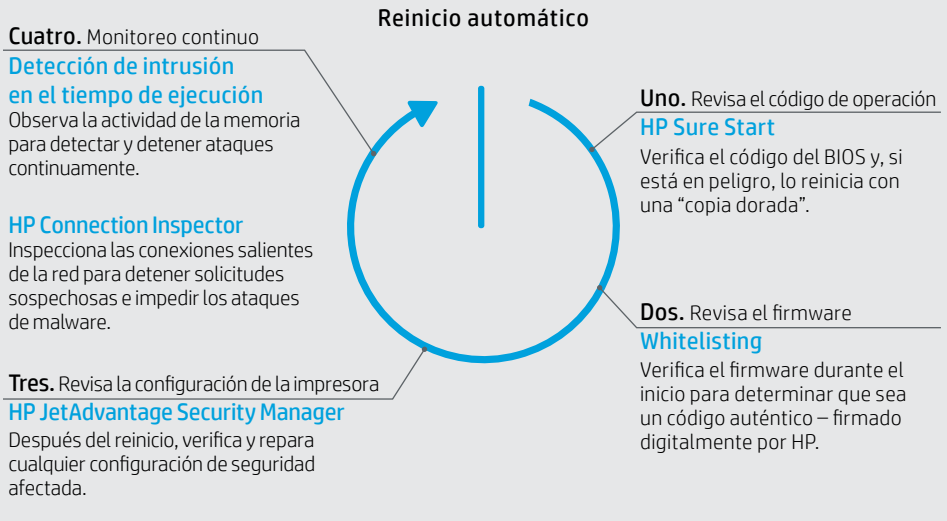
A pesar de estas medidas, Ricoh aún tiene desventajas en comparación con la seguridad completa de HP con su Administrador de Seguridad HP y las funciones que ofrece desde el inicio.

Seguridad de Impresión HP con reparación automática

¿Cómo funciona?
Las características de seguridad cubren cuatro pasos principales en el ciclo de operación de un dispositivo HP.

En caso de un ataque, los dispositivos Enterprise pueden reiniciarse y autorrepararse.

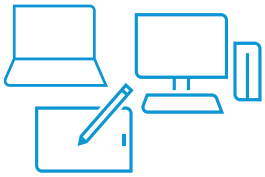
El Administrador de Seguridad HP JetAdvantage completa el ciclo de verificación.



Nueva seguridad integrada: HP Connection Inspector

El diferenciador de seguridad HP más reciente evita que el malware se instale

- Monitorea las conexiones de red salientes (paquetes de datos)
- Aprende lo que es normal e inspecciona y detiene paquetes de datos sospechosos
- Activa un reinicio para comenzar la autorreparación sin necesidad de que TI intervenga

	Ricoh	HP
 **Detección del dispositivo/ whitelisting**	• Ricoh describe sus Soluciones de Seguridad como el acercamiento multinivel que ayuda a cerrarle la puerta a aquellos que quieren atacar las vulnerabilidades. • Se centra en la seguridad estándar de dispositivos heredados como la protección de puertos, autenticación de usuarios, protocolos de red, sobrescritura de datos y cifrado. • No pide escaneo de la memoria contra ataques de inyección. • No proporciona Secure Boot para proteger el código del BIOS en sus dispositivos.	• Excede la oferta de seguridad de Ricoh con capacidades y protecciones integrales, líderes en la industria, incluyendo el BIOS que se repara automáticamente, la integridad del código del firmware y la detección de intrusiones. • Es líder en la industria con la detección de intrusos del dispositivo, que supervisa continuamente la memoria para evitar malware malicioso. • La propuesta de valor de HP FutureSmart protege la inversión del dispositivo, además de ofrecer detección de intrusos y protección de la seguridad a través de actualizaciones de firmware en dispositivos 3.7 FutureSmart desde 2012.
 **Protección de documentos y datos**	• Considera que la educación del usuario final es importante para reducir el riesgo de violación de datos; sin embargo, no proporciona el nivel de tecnología para salvaguardar el equipo, una vez que este tipo de amenaza se encuentra dentro del firewall del dispositivo. • Se centra en los requisitos de seguridad estándar de documentos que están a la par con la industria, pero se queda corto comparado con la seguridad de impresión de HP. • Reconoce que su conjunto completo de características de seguridad no proporciona las protecciones necesarias para eliminar completamente los riesgos causados por errores humanos.	• Ofrece un control de seguridad superior y soluciones de gestión para ayudar a identificar vulnerabilidades, así como establecer un enfoque unificado y basado en políticas para proteger los datos, fortalecer el cumplimiento y reducir el riesgo, todo ahorrando tiempo significativo y recursos. • Supera a Ricoh en la seguridad de extremo a extremo, incluida la supervisión y evaluación de seguridad basadas en políticas, la seguridad Instant–On, la integración SIEM a nivel de dispositivo, la inclusión en la lista de comprobación NIST de los Estados Unidos y la búsqueda de palabras clave DLP.
 **Seguridad de software**	• No cuenta con un proceso Secure Boot que proteja al BIOS. • Brinda validación del firmware únicamente a dispositivos con un chip TPM. • No protege a la memoria contra intromisiones ni al monitor de comportamientos anormales en el tiempo de ejecución del código. • Carece de soluciones robustas y centradas de seguridad, que verifiquen el cumplimiento de las políticas sobre la protección de los dispositivos. • No proporciona detección y análisis de amenazas en tiempo real ni integración con herramientas SIEM como ArcSight o Splunk para proporcionar información sobre posibles ataques. • La oferta de la herramienta de gestión de flotas carece de: 1. Una política de seguridad base que se alinea con los estándares NIST para todos los dispositivos. 2. Un sólido proceso de creación de reglas para afinar políticas de seguridad a las necesidades específicas del cliente. 3. La tecnología Instant-On, que garantiza que las políticas se asignen como dispositivos que se conectan. 4. Corrección automática de hasta 250 configuraciones de seguridad que no cumplen con las políticas definidas.	• Ofrece el Administrador de Seguridad HP JetAdvantage, predecesor en la industria, impulsor de políticas y ganador del premio BLI, vendido, desarrollado y mantenido por HP. • La solución puede evaluar, reportar y remediar a 250 configuraciones, y está diseñada para trabajar con modelos de dispositivos HP 115. • Presenta la tecnología Instant–On, que evalúa automáticamente el cumplimiento de dispositivos HP compatibles.

Preguntas Frecuentes acerca de la seguridad de impresión

P1: Mi empresa utiliza los firewalls para proteger mi red, ¿por qué necesitamos seguridad en nuestras impresoras?

R: ¿Utilizas protección contra malware/virus en tus PCs y portátiles? También tienes que proteger dispositivos de otros equipos en tu red. Si una PC se infecta con malware a través de un correo electrónico con phishing, es poco lo que un firewall puede hacer para proteger los sistemas contra esos casos.

P2: Dada la complejidad de nuestra red y los datos disponibles en nuestros servidores y otros puntos finales, ¿por qué los hackers atacarían las impresoras?

R1: Los hackers no necesariamente atacan los sistemas de forma directa, buscan a las presas más débiles, como una leona va tras la gacela coja del rebaño. Las impresoras son a menudo ignoradas en las políticas de seguridad, por lo que pueden ser como la gacela coja. Una vez que están en tu red pueden acceder a otros recursos, por lo que contar con seguridad del dispositivo de impresión desde el inicio es muy importante.

R2: Las impresoras a menudo procesan, e incluso, almacenan datos sensibles, por lo que podrían ser potentes objetivos para una violación de datos.

P3: ¿Qué sucede si un hacker intenta instalar un malware en mi impresora?

R: Las impresoras HP proporcionan protección contra la instalación de programas maliciosos, incluyendo malware. Nuestra tecnología whitelisting se asegura que solo el código auténtico de HP se instale en el sistema, incluyendo el firmware (el sistema operativo de una impresora) y cualquier otra solución.

P4: ¿Realmente necesitamos toda esta seguridad para nuestras impresoras?

R1: Las impresoras realmente deben ser tratadas como individuos en tu red. Son objetivos para un ataque tan probables como cualquier otro punto de acceso y pueden manejar información altamente sensible con regularidad.

R2: La seguridad requiere constante cuidado, solo se necesita un agujero en tu armadura para ingresar a tus datos, lo que podría costar millones de dólares para que se recupere una empresa.

P5: ¿Cuál es nuestro principal diferenciador en comparación con Ricoh?

R: Nuestra habilidad de reparación automática de potenciales riesgos de seguridad, ya sea a nivel individual del dispositivo con reparación automática o a nivel de la flota a través del Administrador de Seguridad HP JetAdvantage.

Herramientas de evaluación

¿Qué tan seguras son tus impresoras? Evalúa la seguridad de tu entorno de impresión con estas útiles herramientas en línea de HP:

- **Encuesta HP Secure Print Analysis en línea:** autoevaluación para determinar si estás siguiendo las mejores prácticas en seguridad de impresión: hp.com/go/SPA
- **HP Quick Assess:** evaluación técnica gratis de los 13 principales arreglos en hasta 20 impresoras HP (la consulta telefónica está disponible en los Estados Unidos): hp.com/go/quickassess

[1] Fuente: https://www.ricoh.com/security/products/mfp/function/

4AA7-1567SPL, Rev 1, agosto 2018