Información técnica

Cumpla los requisitos normativos relativos a la seguridad de la red y los datos

Recomendaciones para la aplicación de controles de seguridad en su flota de impresión

Contenido

El incumplimiento de la normativa puede perjudicar a su empresa

Además de costosas sanciones y demandas, una brecha en la seguridad de los datos puede hacerle perder ingresos y dañar su reputación. Al crear su plan de seguridad, recuerde que su red es tan segura como su eslabón más débil. Los dispositivos de impresión e imagen experimentan muchas vulnerabilidades en la seguridad similares a las de los ordenadores. Es fundamental la implementación de dispositivos y soluciones que le ayuden a cumplir los requisitos normativos y proteger la información de su empresa frente a las amenazas de seguridad.

¿Cuáles son los riesgos?

La falta de cumplimiento legal y normativo está dando lugar a cuantiosos costes para las organizaciones internacionales, entre los que se incluyen sanciones, pérdida de negocios, reputación dañada y demandas.

Los puntos finales desprotegidos o con una protección insuficiente ofrecen más oportunidades a los ciberdelincuentes. Las organizaciones encuestadas por Ponemon para un estudio reciente sufrieron una media de dos ataques por semana en 2016, lo que supone un incremento del 23 % al año, y pérdidas de una media de 9,5 millones USD anuales en la lucha contra el cibercrimen.[1] Y solo el año pasado, más de 4 mil millones de registros de datos se vieron afectados en todo el mundo, lo que supone un incremento del 400 % con respecto a los dos años anteriores.[2]

Aunque muchos departamentos de TI aplican rigurosas medidas de seguridad en los ordenadores y la red, los dispositivos de impresión e imagen suelen estar desprotegidos. Por ejemplo, las impresoras pueden ofrecer una vía de acceso a la red; de ahí que sea tan importante protegerlas. El 26 % de todas las brechas de seguridad importantes notificadas por los responsables de TI estaba relacionado con sus impresoras.[3]

Para ayudar a contrarrestar la amenaza creciente, las instituciones gubernamentales de todo el mundo están implementando nuevas regulaciones de seguridad estrictas que requieren a las organizaciones proteger mejor la información de los clientes. Por ejemplo, el nuevo Reglamento Europeo de Protección de Datos (GDPR), es una de las leyes más importantes que entrará en vigor en 2018. El GDPR aumenta los requisitos que se exigen a las empresas para proteger sus datos. Por eso es recomendable asegurarse de que todos los dispositivos de la red, desde ordenadores a impresoras y dispositivos móviles, estén protegidos. La nueva ley no solo afecta a los países de la Unión Europea, sino que las empresas internacionales también deben adherirse a ella si recopilan y utilizan datos de residentes de la Unión Europea. Las organizaciones deberán supervisar y evaluar cada dispositivo para detectar e informar sobre infracciones de seguridad en un plazo 72 horas una vez conocida la infracción. Si una auditoría del cumplimiento detecta que las infracciones no han sido supervisadas y que no se ha informado sobre ellas, las empresas se enfrentan a sanciones de hasta los 20 millones de euros o el 4 % de los beneficios anuales de la empresa.

Utilice controles de seguridad comunes para mejorar el cumplimiento

Resulta difícil garantizar el cumplimiento de las normativas legales y sectoriales. Afortunadamente, el Centro de Seguridad en Internet (CIS, por sus siglas en inglés) ha creado una serie de controles de seguridad comunes para simplificar las recomendaciones de seguridad informática. Los Controles de Seguridad Críticos (CSC, por sus siglas en inglés) del CIS consisten en 20 acciones específicas que previenen los ciberataques. (Para obtener más información, visite https://www.cisecurity.org/critical-controls.cfm). Estos controles se ajustan a otras normativas del sector como PCI-DSS, ISO 27001, las recomendaciones de US-CERT, HIPAA, FFIEC y NIST. Los controles no reemplazan a estas otras normativas, pero las empresas los utilizan a menudo para facilitar su aplicación.

Los Controles de Seguridad Críticos del CIS conceden prioridad a un pequeño número de acciones que ofrecen importantes resultados. Combaten los tipos de ataques más habituales según los principales informes sobre amenazas. En su creación ha colaborado un amplio grupo de expertos del sector, que incluye algunos de los principales especialistas en análisis forense y organizaciones de respuesta a incidentes. Además, los controles se actualizan continuamente en función de la evolución de las amenazas y los ataques.

Utilice los Controles de Seguridad Críticos del CIS para organizar su plan de acción de seguridad y cumplir con las normativas. Este documento de información técnica recomienda acciones para cada uno de los 20 controles con el fin de ayudar a proteger sus dispositivos de impresión, la información y los documentos como parte de un plan de seguridad más amplio. Los controles 4, 6, 8, 12, 13 y 15 cubren específicamente la protección de los datos y las actividades de supervisión relativas a los nuevos requisitos de la GDPR.

Controles de Seguridad Críticos del CIS y acciones recomendadas

CSC 1: inventario de dispositivos autorizados y no autorizados

Control: gestione activamente (mediante el inventario, el seguimiento y la corrección) todos los dispositivos de hardware de la red para que únicamente los dispositivos autorizados tengan acceso a ella, a la vez que se detecta e impide el acceso a los dispositivos no autorizados y no gestionados.

Recomendación: asegúrese de que se identifican todos los dispositivos de impresión de la red y de que cuentan con una gestión activa para el cumplimiento de su política de seguridad. Una herramienta eficaz de gestión de la seguridad de impresión detecta y ofrece visibilidad a todos los dispositivos conectados a la red y a ordenadores.

CSC 2: inventario de software autorizado y no autorizado

Control: gestione activamente (mediante el inventario, el seguimiento y la corrección) todo el software de la red para que solo se pueda instalar y ejecutar el software autorizado, a la vez que se detecta e impide la instalación o ejecución del software no autorizado y no gestionado.

Recomendación: asegúrese de que se haya actualizado, firmado y validado la autenticidad de todo el firmware y soluciones cargadas en los dispositivos de impresión e imagen. Elija dispositivos de impresión con protección integrada de la BIOS y el firmware para asegurarse de que solo se cargue código auténtico. Las soluciones de gestión de flotas de impresión permiten la instalación de las actualizaciones del firmware de forma proactiva en toda la flota. El software (tanto instalado en servidores como en clientes) debe estar firmado y tener validada su autenticidad.

CSC 3: configuraciones seguras del hardware y el software de los dispositivos móviles, ordenadores portátiles, estaciones de trabajo y servidores

Control: establezca, implemente y gestione activamente (mediante el seguimiento, los informes y las correcciones) la configuración de seguridad de los ordenadores portátiles, servidores y estaciones de trabajo utilizando un proceso riguroso de gestión de los ajustes y control de los cambios para evitar que los atacantes aprovechen los servicios y configuraciones vulnerables.

Recomendación: al igual que los otros puntos finales de su red, debe configurar las impresoras de forma segura. Es necesario crear e implementar una política de seguridad para todos los dispositivos de impresión y corregir rápidamente cualquier desviación de dicha política. Las listas de comprobación de seguridad (como las que ofrece el NIST) y los servicios de asesoría sobre seguridad pueden ayudarle en el diseño e implementación de una política completa de seguridad de impresión. Una herramienta eficaz de gestión de la seguridad de impresión permite automatizar la creación de políticas, la implementación, la evaluación y la corrección de la configuración de los dispositivos en toda la flota de impresión. Las impresoras multifunción (MFP) para empresas cuentan con más de 250 ajustes de seguridad, por lo que la automatización de este proceso puede suponer un ahorro de tiempo considerable.

CSC 4: evaluación y corrección continua de las vulnerabilidades

Control: recoja datos, evalúelos y actúe continuamente a partir de la nueva información obtenida para identificar y corregir las vulnerabilidades, así como para reducir las oportunidades que tienen los atacantes.

Recomendación: las soluciones de gestión de eventos e información de seguridad (SIEM) como ArcSight, Splunk o SIEMonster, pueden supervisar en tiempo real la actividad de su red y avisar a los administradores cuando se produzcan incidentes. Es tan importante supervisar los dispositivos de impresión como los ordenadores; asegúrese de que sus impresoras pueden enviar mensajes del registro de eventos del sistema a la herramienta de SIEM.

Elija dispositivos de impresión con funciones que permitan la detección de los ataques en tiempo real y la recuperación automática con el fin de aumentar al máximo el tiempo de actividad y reducir las intervenciones del departamento de TI.

Para disminuir las vulnerabilidades, utilice una herramienta de gestión de la seguridad de la flota que pueda identificar las nuevas impresoras y aplicar automáticamente la configuración de la política de seguridad corporativa tan pronto como los dispositivos se conecten a la red. Programe evaluaciones y correcciones periódicas para mantener el cumplimiento de la política en toda su flota de impresión.

CSC 5: uso controlado de los privilegios de administrador

Control: supervise, controle, prevenga y corrija el uso, la asignación y la configuración de los privilegios de administrador en los equipos, redes y aplicaciones.

Recomendación: elija dispositivos y soluciones de impresión que tengan la capacidad de autenticar a los usuarios y controlar el acceso a las funciones según el rol del usuario, de modo que solo el personal de TI o las personas autorizadas puedan instalar y configurar los dispositivos. Use un software de gestión de la seguridad de la flota para establecer contraseñas de administrador en todos los equipos.

CSC 6: mantenimiento, supervisión y análisis de los registros de auditoría

Control: recopile, gestione y analice los registros de auditoría de los eventos que pueden ayudarle a detectar, comprender o recuperarse de un ataque.

Recomendación: los dispositivos de impresión deben tener la capacidad de generar mensajes de registro del sistema respecto a los incidentes para que su equipo de seguridad pueda revisar periódicamente los registros de auditoría con el fin de detectar y solucionar los problemas. Elija dispositivos que puedan enviar estos mensajes a las soluciones de gestión de la seguridad de la flota y las herramientas de SIEM para conseguir una supervisión en tiempo real y la capacidad de generar informes destinados a las auditorías u otros requisitos de cumplimiento.

CSC 7: protecciones del correo electrónico y los navegadores de Internet

Control: reduzca el riesgo de ataques y las oportunidades de que los atacantes manipulen el comportamiento humano cuando se utilizan navegadores de Internet y sistemas de correo electrónico.

Recomendación: las impresoras multifunción están a menudo conectadas a Internet y, por ejemplo, pueden enviar los archivos escaneados por correo electrónico. Asegúrese de que los documentos escaneados que se envían por correo electrónico estén cifrados para proteger los datos confidenciales. Implemente dispositivos y soluciones que permitan la autenticación de los usuarios y el control del acceso a los recursos del dispositivo (como los servidores web o las funciones de correo electrónico) que se basan en los roles de los usuarios. Cree una lista de «sitios de confianza» para sus impresoras multifunción y gestione esta información de forma adecuada para garantizar que solo se pueda acceder a sitios seguros desde los dispositivos. Integre varios métodos de autenticación (como PIN/PIC, LDAP o autenticación Kerberos) con Active Directory para simplificar la gestión y aumentar la seguridad. Los dispositivos de impresión que están conectados a la red deben incluir protección integrada contra el malware y los virus. Además, el firmware de las impresoras debe actualizarse periódicamente para que las últimas protecciones estén en vigor.

CSC 8: defensas contra el malware

Control: controle la instalación, propagación y ejecución de código malicioso en múltiples puntos de su empresa, a la vez que optimiza el uso de la automatización para permitir una rápida actualización de las defensas, la recogida de datos y las acciones correctivas.

Recomendación: elija dispositivos de impresión que solo carguen código verificado y firmado, y que incorporen funciones de protección contra el malware capaces de supervisar activamente la memoria del dispositivo y reiniciarlo en caso de un ataque. Una herramienta eficaz de gestión de la seguridad de impresión permite automatizar la evaluación y la corrección de la configuración de los dispositivos en toda la flota de impresión. También debe asegurarse de que todas las soluciones de software de impresión estén firmadas y validadas como auténticas.

CSC 9: limitación y control de los puertos, protocolos y servicios de red

Control: gestione (mediante el control, la supervisión y la corrección) el uso actual de los puertos, protocolos y servicios de los dispositivos en red con el fin de reducir las vulnerabilidades que pueden aprovechar los atacantes.

Recomendación: si no están desactivados de forma predeterminada, deshabilite los puertos que no se usan y los protocolos no seguros (como FTP o Telnet) que los atacantes pueden utilizar para acceder al dispositivo. Ahorre tiempo al departamento de TI y disminuya los riesgos con la implementación de una herramienta de gestión de la seguridad de impresión que permita mantener automáticamente la configuración de cada dispositivo de acuerdo con la política de la flota. Utilice contraseñas de administrador, funciones de autenticación y controles de acceso basados en roles para limitar el acceso a las funciones y la configuración del dispositivo.

CSC 10: funciones de recuperación de datos

Control: haga copias de seguridad de la información importante mediante un método probado que permita recuperar los datos con rapidez.

Recomendación: este control no se aplica actualmente a las impresoras.

CSC 11: configuraciones seguras de los dispositivos de red como cortafuegos, enrutadores y conmutadores

Control: establezca, implemente y gestione activamente (mediante el seguimiento, los informes y las correcciones) la configuración de seguridad de los dispositivos de infraestructura de red con un proceso riguroso de gestión de la configuración y control de los cambios para evitar que los atacantes aprovechen los servicios y configuraciones vulnerables.

Recomendación: las impresoras forman parte de su red y, al igual que los otros puntos finales, debe configurarlas de forma segura. Una herramienta eficaz de gestión de la seguridad de impresión permite automatizar la implementación, la evaluación y la corrección de la configuración de los dispositivos en toda la flota para mantener segura la red y ahorrar tiempo al departamento de TI.

CSC 12: defensa perimetral

Control: detecte, prevenga y corrija el flujo de información que se transmite entre redes con diferentes niveles de confianza y con un énfasis especial en los datos potencialmente dañinos para la seguridad.

Recomendación: utilice el cifrado para proteger los datos que se transmiten (trabajos de impresión o de escaneado que se envían a la impresora o desde ella) y los datos almacenados en el disco duro del dispositivo. Elija dispositivos y soluciones de impresión con la capacidad de autenticar a los usuarios y controlar el acceso a las funciones según el rol de los usuarios. Por ejemplo, puede hacer que solo los usuarios autorizados puedan enviar trabajos de escaneado por correo electrónico o enviar archivos a destinos en la nube. Configure los sitios web de confianza en la lista de «sitios seguros» del dispositivo para impedir el acceso a páginas peligrosas. Las soluciones de impresión móvil segura pueden facilitar a los usuarios la impresión desde sus dispositivos móviles al mismo tiempo que protegen la red.

CSC 13: protección de la información

Control: prevenga las filtraciones de datos, mitigue sus efectos cuando se produzcan y garantice la privacidad e integridad de la información confidencial.

Recomendación: utilice el cifrado para proteger los datos que se transmiten (trabajos de impresión o de escaneado que se envían a la impresora o desde ella) y los datos almacenados en el disco duro del dispositivo. Implemente soluciones de impresión pull para evitar que queden documentos confidenciales sin recoger en las bandejas de salida. Asegúrese de que los datos almacenados en los discos duros de los dispositivos se borren de forma segura antes de devolver los dispositivos arrendados o de reciclarlos al final de su vida útil.

CSC 14: control del acceso según la necesidad de información

Control: realice un seguimiento, control, prevención, corrección y protección del acceso a los activos importantes (como la información, recursos y sistemas) mediante la determinación formal de qué personas, ordenadores y aplicaciones tienen la necesidad y el derecho de acceder a ellos según una clasificación aprobada.

Recomendación: elija dispositivos y soluciones de impresión que tengan la capacidad de autenticar a los usuarios y controlar el acceso a las funciones según el rol del usuario. Integre varios métodos de autenticación (como PIN/PIC, LDAP o autenticación Kerberos) con Active Directory para simplificar la gestión y aumentar la seguridad. Las soluciones de impresión pull pueden evitar que los documentos confidenciales caigan en las manos equivocadas.

CSC 15: control del acceso inalámbrico

Control: realice un seguimiento, control, prevención y corrección del uso seguro de las redes de área local inalámbricas (WLAN), los puntos de acceso y los sistemas cliente inalámbricos.

Recomendación: una herramienta eficaz de gestión de la seguridad de impresión permite automatizar la implementación, evaluación y corrección de la configuración de los dispositivos (incluidas las funciones inalámbricas) en toda la flota. Utilice soluciones de control de acceso para restringir el acceso a determinadas funciones de los dispositivos, como el escaneado a correos electrónicos, en función del rol del usuario. Las soluciones de impresión móvil segura pueden facilitar a los usuarios la impresión desde sus dispositivos móviles, al mismo tiempo que protegen la red. Por ejemplo, los dispositivos que admiten la impresión inalámbrica de punto a punto permiten a los usuarios móviles imprimir directamente usando la señal inalámbrica propia de la impresora, sin acceder a la red o a los servicios inalámbricos de la empresa.

CSC 16: supervisión y control de cuentas

Control: gestione activamente el ciclo de vida de las cuentas de los sistemas y aplicaciones (creación, uso, vigencia y cancelación) para reducir las oportunidades de que los atacantes se aprovechen de ellas.

Recomendación: elija dispositivos y soluciones de impresión que tengan la capacidad de autenticar a los usuarios y controlar el acceso a las funciones según el rol del usuario. Integre la autenticación con Active Directory para una gestión centralizada y una mayor seguridad. Revise regularmente las cuentas de los usuarios y desactive las que sean innecesarias, además de utilizar soluciones de seguimiento para la supervisión del uso de las cuentas. Cifre los nombres de usuario y las credenciales de autenticación de las cuentas cuando se transmitan o se almacenen en los dispositivos. Los consultores de seguridad pueden ayudarle a diseñar un plan completo de seguridad de impresión para reducir los riesgos y, en algunos casos, pueden colaborar en la gestión de la seguridad, incluida la supervisión y el control de cuentas.

CSC 17: evaluación de las habilidades de seguridad y formación adecuada para cubrir las carencias

Control: identifique los conocimientos, habilidades y capacidades específicas necesarias para mejorar la seguridad de su empresa; desarrolle y ponga en marcha un plan integrado para la evaluación, identificación y resolución de las carencias mediante políticas, planificación organizacional, formación y programas de concienciación para todos los roles funcionales de la empresa.

Recomendación: los consultores de seguridad de impresión tienen el conocimiento especializado necesario para ayudarle a evaluar sus riesgos de seguridad, desarrollar una política y un plan de seguridad integral, e implementar los procesos y tecnologías recomendados. Algunos servicios de seguridad pueden incluso gestionar la seguridad y el cumplimiento de la impresión en su lugar.

CSC 18: seguridad del software de aplicación

Control: gestione el ciclo de vida de seguridad de todo el software desarrollado internamente y adquirido para prevenir, detectar y corregir las vulnerabilidades de seguridad.

Recomendación: siga las prácticas recomendadas de desarrollo seguro en todas las soluciones de impresión desarrolladas. Elija soluciones de software que se hayan firmado y validado como auténticas.

CSC 19: respuesta y gestión de los incidentes

Control: proteja la información y la reputación de su empresa mediante el desarrollo e implementación de una infraestructura de respuesta a los incidentes (por ejemplo, planes, funciones definidas, formación, comunicaciones y supervisión de la gestión).

Recomendación: verifique que su entorno de impresión se incluya en su plan de respuesta a los incidentes de seguridad.

CSC 20: pruebas de penetración y ejercicios de Red Team

Control: ponga a prueba la solidez global de las defensas de su empresa (tecnología, procesos y usuarios) mediante la simulación de los objetivos y las acciones de un atacante.

Recomendación: incluya su entorno de impresión en la realización de las pruebas de penetración. Evalúe periódicamente su entorno de impresión en busca de vulnerabilidades y actualice su plan de seguridad para resolver las deficiencias detectadas.

Dé el siguiente paso

La implementación de las recomendaciones que ofrece este documento de información técnica puede ayudarle a reforzar la seguridad de impresión y cumplir las normativas. ¿Necesita ayuda? Los servicios de gestión y asesoría sobre seguridad de impresión le asisten en el desarrollo de una planificación y en la implementación de procesos y tecnologías que mejoran la seguridad de sus dispositivos de impresión, información y documentos.

Anexo A: funciones, soluciones y servicios de seguridad de impresión de HP

Las funciones de seguridad integradas en los dispositivos de HP, junto con las soluciones y servicios de software líderes del sector, pueden ayudarle en el cumplimiento de los requisitos legales y sectoriales, así como en la protección de la información de su empresa frente a las amenazas de seguridad.

Las funciones de seguridad integradas en las impresoras e impresoras multifunción para empresas de HP ofrecen protección contra el malware y permiten la detección y recuperación automática en caso de un ataque. Solo la seguridad de impresión de HP ofrece funciones de detección en tiempo real, supervisión automatizada y validación de software integrada para detener las amenazas en el momento en que se inician.[4] (Facilita el cumplimiento de CSC 2, 4, 6 y 8). hp.com/go/PrintersThatProtect

Las soluciones de HP Access Control proporcionan una serie de funciones de autenticación y control de acceso basado en roles para reducir las brechas de seguridad potenciales, además de permitir el seguimiento y la contabilidad de los trabajos. (Facilita el cumplimiento de CSC 5, 7, 10, 12, 13, 14, 15 y 16). hp.com/go/hpac

Las soluciones de cifrado y de flujo de trabajo de HP JetAdvantage protegen los datos cuando se almacenan en los dispositivos para empresas de HP y cuando se transmiten de o hacia los dispositivos de impresión o la nube. (Facilita el cumplimiento de CSC 12 y 13). hp.com/go/upd, hp.com/go/documentmanagement

Las soluciones de impresión pull de HP protegen los documentos confidenciales mediante el almacenamiento de los trabajos de impresión en un servidor protegido, en la nube o en su ordenador. Los usuarios se autentican en la ubicación de impresión elegida para recuperar e imprimir sus trabajos. (Facilita el cumplimiento de los CSC 10, 13 y 14). hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect ofrece a los usuarios móviles un acceso fácil a la impresión desde smartphones y tablets, a la vez que permite el mantenimiento de la seguridad y el control administrativo que necesita. (Facilita el cumplimiento de CSC 12 y 15). hp.com/go/JetAdvantageConnect

Los datos de los eventos de las impresoras HP se pueden integrar con herramientas de SIEM como ArcSight, Splunk o SIEMonster. El equipo de seguridad puede controlar fácilmente los puntos finales de las impresoras como parte del amplio ecosistema tecnológico de la empresa y adoptar medidas correctoras. (Facilita el cumplimiento de CSC 4 y 6).

HP JetAdvantage Security Manager es la única herramienta de cumplimiento de la seguridad de impresión basada en políticas.[5] Le permite el establecimiento de una política de seguridad para toda la flota, la automatización de la corrección de los ajustes de los dispositivos y la instalación y renovación de certificados únicos, a la vez que obtiene los informes que necesita para acreditar el cumplimiento. La función Instant-On de esta solución configura automáticamente los nuevos dispositivos cuando se añaden a la red o después de un reinicio. (Facilita el cumplimiento de CSC 1, 2, 3, 4, 5, 6, 8, 9, 11 y 15). hp.com/go/securitymanager

Los servicios gestionados de impresión segura de HP proporcionan la seguridad de impresión más sólida y completa del sector.[6] La seguridad de impresión puede ser un asunto complicado. Deje que HP gestione su seguridad de impresión, desde la mejora de la protección de los dispositivos hasta la instalación de soluciones de seguridad avanzadas dirigidas a los usuarios, a los procesos y al cumplimiento. (Facilita el cumplimiento de CSC 2, 3, 12, 16, 17, 18 y 19). hp.com/go/SecureMPS

Los servicios profesionales de seguridad de impresión de HP proporcionan expertos en seguridad que le ayudan a evaluar su entorno de impresión, establecer de manera proactiva las políticas de seguridad y mantener actualizado su plan de seguridad. Podemos incluso gestionar la seguridad y el cumplimiento de la impresión por usted. (Facilita el cumplimiento de CSC 2, 3, 12, 16, 17 y 19). hp.com/go/SecureMPS

Notas

[1] Estudio del Instituto Ponemon patrocinado por HPE, «2016 Cost of Cyber Crime Study & the Risk of Business Innovation» (2016 Estudio del coste de los delitos informáticos y el riesgo de la innovación empresarial), 2016.

[2] Informe «The 2016 Year End Data Breach QuickView» por RiskBased Security, enero de 2017.

[3] El 26,2 % de los encuestados sufrió una brecha importante en la seguridad de TI que necesitó una corrección y más del 26,1 % de estos incidentes estuvo relacionado con la impresión. IDC: «Encuesta de seguridad de impresión y TI de 2015», n.º US40612015, septiembre de 2015.

[4] Se aplica a los dispositivos HP de categoría empresarial presentados a partir de 2015 y se basa en el análisis de HP de la información publicada en 2016 sobre las funciones de seguridad integradas en las impresoras de la competencia de la misma categoría. Solo HP ofrece una combinación de funciones de seguridad que comprueba la integridad de la BIOS con capacidades de recuperación automática. Para activar las funciones de seguridad, es posible que se necesite una actualización del paquete de servicios FutureSmart. Para consultar la lista de productos compatibles, visite hp.com/go/PrintersThatProtect. Para obtener más información, visite: hp.com/go/printersecurityclaims.

[5] HP JetAdvantage Security Manager se vende por separado. Para obtener más información, visite hp.com/go/securitymanager. Basado en estudios internos relativos a ofertas de la competencia de HP (Comparativa de seguridad de dispositivos de enero de 2015) y el informe sobre las soluciones de HP JetAdvantage Security Manager 2.1 realizado por Buyers Laboratory, LLC. en febrero de 2015.

[6] Incluye soluciones de seguridad para los dispositivos, información y documentos ofrecidas por proveedores líderes de servicios gestionados de impresión. Basado en el análisis realizado por HP de la información publicada en 2015-2016 sobre los servicios de seguridad, el software de seguridad y gestión, y las funciones de seguridad integradas en las impresoras de la misma categoría de la competencia. Para obtener más información, visite hp.com/go/MPSsecurityclaims o hp.com/go/mps.

Suscríbase para recibir novedades
hp.com/go/getupdated

Compartir con compañeros

4AA6-8821ESE, Junio de 2017, rev. 1