Artículo técnico sobre seguridad de la información

Seguridad de las redes

Protección para los dispositivos de red de la oficina

SHARP
Be Original.

www.sharp.es

Contenido

Introducción

En el mundo conectado de hoy en día, garantizar la seguridad efectiva de la información en toda la red de la empresa nunca ha sido tan vital.

Todos los días se producen incontables intentos maliciosos de robar, modificar ilegalmente, interceptar o diseminar documentos confidenciales, u obtener acceso no autorizado a redes privadas y empresariales. En este artículo técnico se examinan los principales desafíos a los que se enfrentan las empresas a la hora de proteger sus infraestructuras de TI en relación con los dispositivos de oficina conectados a la red, como las impresoras estándar y las impresoras multifunción.

En este artículo técnico se examinará:

- **El contexto**
  Todas las empresas se enfrentan a desafíos desde el punto de vista de la seguridad de la red, pero, a menudo, se suelen pasar por alto las vulnerabilidades a las que se exponen las impresoras estándar y las impresoras multifunción conectadas a la red. Los piratas informáticos y los cibercriminales las suelen utilizar como vía de acceso a las organizaciones para robar datos confidenciales almacenados en discos duros y otros dispositivos en red, así como para causar daños o alterar las actividades empresariales. El impacto en la productividad y la rentabilidad puede ser enorme.

- **El problema**
  El riesgo que platean las impresoras estándar y las impresoras multifunción no seguras se suele comprender mal o ignorar. También puede ocurrir simplemente que las empresas no cuentan con el conocimiento y los recursos necesarios para atajar el problema. Asimismo, el desconocimiento de los usuarios exacerba esta cuestión, pues las malas prácticas exponen innecesariamente documentos y datos al riesgo de verse comprometidos. Las empresas entienden los pasos que necesitan dar para crear una política de seguridad de impresión, pero el proceso puede ser complejo y exigir mucho tiempo.

- **Las recomendaciones**
  Describimos un conjunto de soluciones de hardware y software, así como prácticas recomendadas que pueden ayudarle a desarrollar un entorno de impresión seguro y evitar accesos no autorizados y ataques a los dispositivos conectados a la red. Esa sección incluye respuestas específicas a algunos de los principales desafíos de seguridad:

  - Seis pasos dirigidos a introducir y mantener los estándares de seguridad de impresión con ayuda de una combinación de tecnologías y soluciones de software optimizadas de Sharp.
  - Funciones y ajustes de serie incluidos en todos los dispositivos Sharp conectados de la gama actual, por ejemplo, protección con contraseña, sobreescritura de los datos, cifrado, etc.
  - Soluciones opcionales que le ayudan a desarrollar una política de seguridad de impresión uniforme y a gestionar flotas de impresoras de forma sencilla y eficaz, por ejemplo, el gestor de dispositivos remotos de Sharp (SRDM)
  - Funciones y características avanzadas opcionales para impresoras estándar e impresoras multifunción, por ejemplo, el kit de seguridad de datos (DSK)
  - Servicios opcionales disponibles a través del canal directo de Sharp, por ejemplo, auditorías de seguridad, seguridad como servicio, eliminación de datos al final de ciclo de vida, etc.

- **La conclusión**
  Proporcionamos un resumen de lo siguiente:

  - Los hallazgos sobre vulnerabilidades empresariales en relación con cada impresora estándar e impresora multifunción conectada a la red
  - Nuestras recomendaciones se basan en funciones integradas y soluciones de seguridad adicionales de Sharp
  - Los siguientes pasos requeridos para desarrollar una política de seguridad de impresión, ya sea sobre la base de un enfoque interno o con la ayuda o la experiencia del equipo de servicios profesionales de Sharp.

Contexto

La necesidad de seguridad efectiva de TI ha cobrado mayor relieve en los últimos años, pero se ha pasado peligrosamente por alto un área fundamental.

Las organizaciones conscientes de la seguridad se han asegurado de que sus activos informáticos y de red estén protegidos con la última tecnología mediante la instalación de cortafuegos, la aplicación de reglas de contraseña, la exigencia de autenticación de los usuarios, la protección de datos cifrados y firmados electrónicamente, etc.

Nuevas tecnologías, como la nube y las comunicaciones móviles, han planteado desafíos adicionales para los administradores de TI y los responsables de seguridad. Sin embargo, las impresoras estándar y las impresoras multifunción han evolucionado para incluir muchas comunicaciones de red y capacidades de almacenamiento de datos. Básicamente, se han convertido en potentes ordenadores con funciones inteligentes. Según IDC, hay casi 53 millones de impresoras y dispositivos multifunción en oficinas y hogares de toda Europa oriental y occidental[1], y la mayor parte de ellas están conectadas a una red. Este hecho las convierte en un punto de acceso con una dirección IP y son tan susceptibles al malware y a los ataques de piratas informáticos como los ordenadores y otros terminales conectados a una red. Por lo tanto, requieren el mismo nivel de funciones de seguridad de datos, comunicación e información.

El 25 % de las violaciones de la seguridad de TI que requirieron intervención tuvieron que ver con la impresión.[2]

Si las impresoras multifunción se dejan sin proteger, los piratas informáticos pueden acceder a puertos y protocolos no controlados, lo que podría brindarles acceso, a su vez, a otras máquinas de la red o a información confidencial. Las comunicaciones y los datos almacenados en los discos duros o las memorias de las impresoras multifunción pueden ser interceptados o enviados sin permiso a cualquier parte del mundo. Los dispositivos en red también podrían ser objeto de ataques de denegación de servicio (DoS), cuyo objetivo es impedir el acceso a los recursos de red a los usuarios finales, con el consiguiente impacto en la productividad de la empresa. También pueden proporcionar una vía de acceso para ataques de suplantación de identidad diseñados para obtener información confidencial o introducir virus en la red.

No se trata una moda, sino de una amenaza real. Según un reciente estudio de IDC, más de un 25 % de los encuestados admitieron haber sido objeto de una violación de la seguridad de TI importante que requirió intervención, y más del 25 % de estos incidentes tuvo que ver con la impresión.[2]

No proteger las impresoras estándar o las impresoras multifunción puede dar lugar a daños devastadores para una empresa, además de para su reputación y la confianza de los clientes. Entre los efectos de una infracción se incluyen:

- Pérdidas de ingresos
- Pérdidas de productividad por la falta de acceso a datos y a la red
- Pérdida de competitividad debido a información robada
- Multas por el incumplimiento de normativas
- Demandas judiciales
- Uso no autorizado de equipos y recursos de red.

Problema

Las actividades de los piratas informático y los ciberataques se han convertido en la «norma» y, con independencia del tipo y el tamaño de la empresa, la amenaza de la actividad de malware que afecta a las operaciones es muy real e inminente.

Puede sorprenderle, pero, según la empresa Quocirca, el 63 % de las empresas encuestadas admiten haber experimentado una o varias violaciones de la seguridad relacionadas con las impresión[3].

Cabe preguntarse por qué no han hecho nada las empresas para combatir la amenaza.

Por desgracia, el riesgo potencial se suele pasar por alto debido a la falta de comprensión de las vulnerabilidades que surgen cuando se introducen impresoras estándar e impresoras multifunción en la red de la empresa. Muchas empresas no cuentan con sistemas ni herramientas de seguridad de impresión, o los medios que utilizan son insuficientes, como personal formado, prácticas recomendadas y procedimientos de seguridad relacionados con el uso de dispositivos conectados a la red. O utilizan dispositivos para fines empresariales diseñados, de hecho, para uso doméstico, y con funciones de seguridad limitadas.

En concreto, muchas pequeñas y medianas empresas no han introducido ninguna medida de seguridad de las impresiones o no han realizado nunca una auditoría de seguridad de impresión. Y las organizaciones más grandes a veces no cuentan con recursos humanos insuficientes, o la calidad de las herramientas para la medición, control y prevención de los ataques de seguridad sobre los dispositivos de red y tecnologías conectadas puede dejar mucho que desear.

Además, las malas prácticas de usuario suelen plantear un grave desafío para los administradores de TI, pues pueden causar importantes problemas de seguridad para las empresas. Entre ellas, se incluyen imprimir información de forma no segura, dejar documentos sin atender en las bandejas de salida de la impresora estándar o la impresora multifunción, imprimir desde memorias USB no seguras, no aplicar cifrado de extremo a extremo al imprimir o almacenar documentos sensibles en el disco duro de la impresora estándar o la impresora multifunción.

Para muchas empresas, la eliminación de los datos a la finalización de un contrato también

Casi dos tercios de las empresas han experimentado una violación de la seguridad relacionada con la impresión.[3]

puede plantear un problema. El proceso de impresión puede dejar copias de los datos que se han impreso dentro del disco duro del dispositivo. Cabe preguntarse qué ocurre con los datos cuando finaliza el contrato.

Por desgracia, configurar un sistema homogéneo de seguridad de las redes o introducir una política de seguridad de impresión destinado a detectar y evitar accesos no autorizados a una flota de impresoras estándar o impresoras multifunción conectadas en red puede resultar complejo y requerir mucho tiempo. Es muy probable que necesite pasar por las siguientes fases clave:

- Predecir y evaluar cualquier posible implicación resultante de no contar con un sistema de seguridad de las redes
- Reconocer la existencia de posibles vulnerabilidades y los daños que podrían ocasionar en la infraestructura de red
- Entender la complicada naturaleza del desafío, que variará inevitablemente de una empresa a otra
- Encontrar un recurso interno o externo que le ayude a abordar el desafío
- Identificar herramientas capaces de supervisar flotas enteras de impresoras estándar o impresoras multifunción, evitar accesos no autorizados a los activos conectados a la red y obtener alertas de cualquier actividad sospechosa
- Instalar y mantener un sistema de seguridad de las redes fiable que aborde el conjunto especial de desafíos a los que se enfrentan las empresas

Recomendaciones

Si todo lo que le hemos contado hasta ahora le ha llevado a dudar de la seguridad de su red, tranquilo. El riesgo para la empresa no debe subestimarse, pero no debe tener miedo.

Nuestro objetivo es presentar una forma sencilla de introducir medidas completas de seguridad de las impresiones en su empresa y explicarle cómo puede ayudarle Sharp a entender y elevar sus niveles de seguridad de las redes fácilmente y sin dificultad.

Protección instantánea

Según investigaciones realizadas por la empresa de análisis de la industria IDC, «los proveedores de tecnologías de servicios de documentos e impresiones en papel están concentrando sus esfuerzos en la seguridad de los dispositivos de impresión para impedir que los piratas informáticos accedan a las redes empresariales a través de ellos».[4] Sin embargo, muchas empresas pasan por alto o no establecen los ajustes de seguridad adecuadamente, lo que puede dejarlas vulnerables a ataques.

La siguiente es una lista de funciones y ajustes de seguridad comercializados de serie en todas las impresoras estándar e impresoras multifunción de Sharp, que pueden proporcionar una solución rápida. Todos ellos se pueden activar o desactivar rápidamente o el administrador de red puede ajustarlos para cambiar los niveles de seguridad predeterminados y proporcionar una protección mucho más efectiva para las necesidades concretas de su empresa:

- Ajustes locales de administración incluidos: cambio de la contraseña de administrador, acceso a la página web del dispositivo y seguridad para uso remoto
- Configuración de las funciones de seguridad de modo estándar: controles de puerto, ajustes de protocolo, ajustes de SNMP MIB, filtros de acceso, SSL, S/MIME, IPSEC, IEEE802.1X, activación/desactivación de protocolos de impresión móviles, ajustes de servicio externo, carpeta pública - servidor con dirección de red (disco compartido), ID de seguimiento, ajustes de usuario, activación/desactivación de soluciones de seguridad de usuario, eliminación automática de archivos almacenados y eliminación de cola de impresión en caso de error
- Funciones avanzadas de seguridad (en modo de seguridad estándar): sobreescritura de los datos del disco duro (borrado del disco duro) tras cada tarea de copia, impresión, digitalización o envío de fax, cifrado de almacenamiento y protección con contraseña
- En el mismo grupo hay varios ajustes avanzados opcionales. Estos ajustes ofrecen a los administradores de TI acceso a funciones de seguridad avanzadas de Sharp que ofrecen ventajas para las organizaciones que precisan los niveles de seguridad más altos, como organismos militares y gubernamentales, o cualquier empresa que desee elevar su seguridad al nivel más alto:

  - El kit de seguridad de datos (DSK) incluye: instalación del kit de seguridad de datos, mejoras de seguridad de datos, mejoras de seguridad para la impresión y validación del firmware
  - El kit avanzado de seguridad de datos (DSK avanzado) incluye: modo de seguridad avanzado con certificación HCD-PP (incluye el kit de seguridad de datos), cifrado mejorado del almacenamiento, requisito de contraseña mejorada y comprobaciones de seguridad del firmware

Seis pasos sencillos

Desde una perspectiva de seguridad a más largo plazo, los siguientes seis pasos ofrecen una forma estructurada de desarrollar e introducir un marco homogéneo propio para la seguridad de las redes.

1. **Acceso seguro a la red**
   Cualquier dispositivo conectado es tan seguro como el punto más vulnerable de la red. Por lo tanto, controlar el uso de los puertos y los protocolos es una parte muy importante para garantizar la seguridad de las redes. A través de configuraciones seguras, los administradores de TI pueden evitar actividades no deseadas y ataques potenciales sobre la infraestructura. Entre las técnicas para garantizar las comunicaciones seguras entre cada dispositivo y la red, se incluyen:

   - El uso de filtrado IP para limitar el acceso a direcciones IP específicas, así como filtrado MAC (control de acceso a medios). Esta técnica le ayuda a proteger su red y sus canales de comunicación mediante el acceso a través de direcciones o intervalos de IP específicos.
   - La desactivación de puertos no utilizados (de forma que solo funcionen los requeridos) proporciona una capa de seguridad adicional y ofrece un mayor

control sobre la red, pues impide el acceso no autorizado al conjunto de activos conectados.
- Configurar IPSec (la seguridad del protocolo de Internet para el intercambio seguro y cifrado de datos), TLS (la seguridad de la capa de transporte para la transmisión de datos cifrados) y HTTPS (la seguridad del protocolo de transferencia de hipertexto para comunicaciones seguras de red) en el máximo nivel de protección.

2. Protección del dispositivo (para garantizar la seguridad de los datos)
Existen dos formas de garantizar la seguridad de los datos almacenados en los discos duros de las impresoras estándar y las impresoras multifunción:

- El cifrado de datos es el procedimiento o funcionalidad que cifra los documentos mediante un algoritmo complejo de 256 bits.
- La sobreescritura es la opción consistente en borrar los datos del disco duro de un dispositivo. Este método se asegura de que todos los datos y las imágenes electrónicas de documentos impresos almacenados en el disco duro se borran sobreescribiéndolos hasta 10 veces.

Para mayor tranquilidad, Sharp también ofrece una opción de servicio de final de vida útil que garantiza la eliminación de cualquier dato digital que quede en un dispositivo y la destrucción del disco duro.

3. Acceso seguro de usuario (a través de identificación y autorización de usuario)
Uno de los pasos más importantes consiste en controlar a todos los usuarios mediante la introducción de funciones de administración y autorización de usuarios. En esta categoría las principales actividades consisten en:

- La identificación de usuarios es un proceso a través del cual los administradores solo conceden derechos de acceso a las impresoras estándar y las impresoras multifunción a los usuarios registrados. Deben identificar a los usuarios a través autenticación local, basada en la lista de usuarios locales, o autenticación de red a través del servidor de autenticación.

- La autenticación de usuarios se utiliza para conceder acceso a los recursos en red de la organización y controlar su uso. Sobre la base de credenciales de cada usuario, pueden limitar el acceso a personas específicas, restringirlo a funciones de dispositivo o bloquearlo completamente. Los administradores también pueden configurar el acceso al dispositivo a través de tarjetas de identidad, que almacenan los datos de identificación del usuario.

4. Impresión segura de información confidencial
Los documentos confidenciales solo deben imprimirse mediante un procedimiento seguro que evite accesos y copias no autorizadas. Por regla general, cuando se envía un trabajo de impresión, este se almacena en el disco duro del dispositivo y solo se libera cuando el usuario introduce un código PIN, configurado previamente. Una vez impreso el documento, todos los datos se borran automáticamente del disco duro.

5. Control de la actividad de red
Cuando se introducen correctamente, las herramientas de seguridad de las redes pueden ofrecer a los administradores de TI un control total de todos los dispositivos en red, directamente desde sus escritorios, para permitirles controlar una flota entera de impresoras estándar e impresoras multifunción, así como descubrir, configurar y gestionar la mayor parte de las amenazas potenciales de seguridad. La capacidad para clonar dispositivos también simplifica el trabajo de los administradores y proporciona mayor tranquilidad, ya que cualquier cambio realizado en los ajustes de una máquina puede propagarse de forma sencilla a toda la flota.

6. Selección del socio adecuado
Son muchas las empresas que ofrecen servicios profesionales relacionados con la seguridad de las impresiones. Sin embargo, el nivel de experiencia puede variar considerablemente. Sharp se toma la seguridad de la red muy en serio y es un elemento fundamental en cualquier innovación de producto. Como fabricante, nuestros equipos se evalúan sobre la base de las directrices especificadas en la completa certificación Common Criteria. Como resultado, nuestras impresoras multifunción en red con una opción de seguridad de datos integrada han sido evaluadas de manera independiente por el reconocido JISEC (Sistema de Evaluación y Certificación de Seguridad de TI) de Japón. Nuestras impresoras cuentan con el último certificado HCD-PP v1.0 (Perfil de Protección de Dispositivos de Impresión, versión 1.0) de los Common Criteria, lo que nos permite ayudar a los clientes a gestionar los datos más confidenciales del mundo.

Obtenga ayuda externa

Aunque la tarea pueda parecer abrumadora, es importante recordar que no está solo, pues tiene a su disposición ayuda experta en todo momento.

En concreto, Sharp ofrece varias soluciones, herramientas y servicios para comprobar y medir las vulnerabilidades de su red, preparar un plan de mejora y diseñar posibles escenarios:

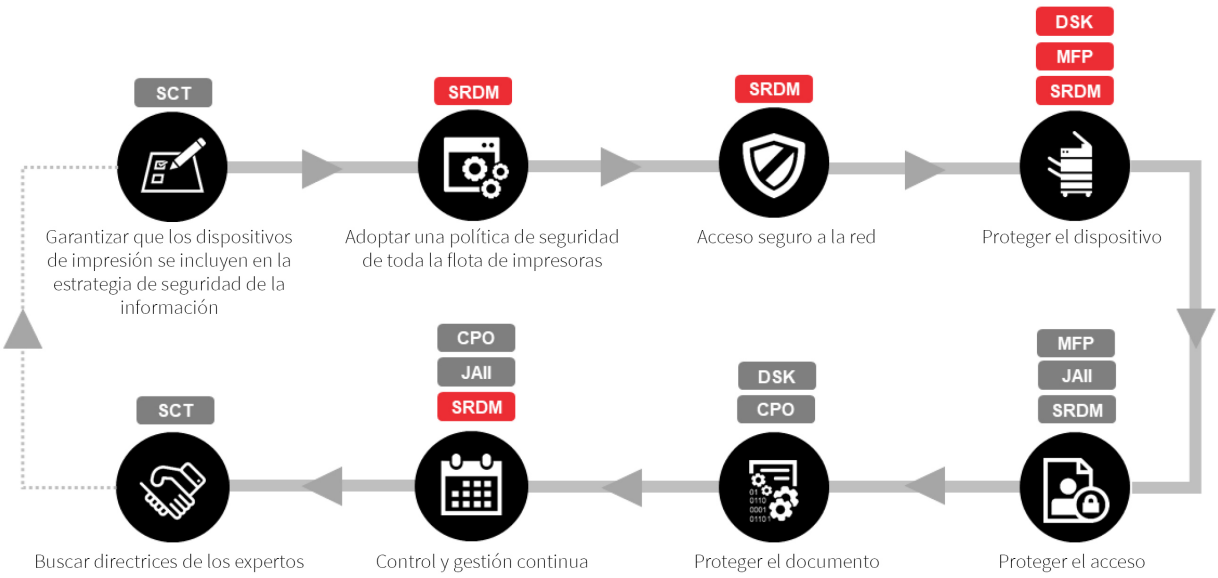
- **Taller de seguridad de impresión**
  Podemos aprovechar un conjunto de herramientas y técnicas para ayudarle a entender las amenazas de seguridad, enumerar las conclusiones y desarrollar un plan de mejora ajustado.

  La auditoría se centra en todos los periféricos conectados en red y su seguridad. Medimos todas las funciones estándar y avanzadas disponibles para estos dispositivos, así como las herramientas para el descubrimiento y la prevención efectivas de amenazas. También comprobamos si los dispositivos que utiliza en su empresa son adecuados para su fin y podemos ofrecer máxima protección de seguridad para su empresa y sus usuarios. Además, la auditoría de seguridad de impresión incluye los «siguientes pasos» para introducir una política de seguridad de impresión y abarca todos los aspectos de seguridad de su empresa, incluidos los siguientes:
  - Seguridad de las redes, como se describe en este documento
  - Seguridad de las salidas, que abarca todas las actividades relacionadas con la salida de documentos, como impresión, digitalización, envío por fax y envío por correo electrónico
  - Seguridad de documentos, que aborda la gestión de los archivos electrónicos y en papel utilizados en su oficina
  - Cumplimiento del RGPD, que garantiza la conformidad con las últimas normativas de la UE sobre seguridad y protección de los datos personales

- **Paquete de seguridad**
  Aquí se combina un taller del cliente con la instalación del gestor de dispositivos remotos de Sharp, así como el despliegue y la configuración opcional del sistema de gestión de las salidas para abarcar mayores parcelas de seguridad de la oficina: seguridad de las redes y seguridad de las salidas.

- **Gestor de dispositivos remotos de Sharp (SRDM)**
  Esta herramienta de Sharp ayuda a introducir ajustes de seguridad esenciales en cuestión de segundos. La implementación se realiza en forma de servicio por parte de un equipo capacitado de Sharp. Sobre la base de sus necesidades y requisitos, se pueden introducir todos los ajustes de seguridad pertinentes y todas las impresoras estándar y las impresoras multifunción de Sharp estarán bajo control.

Desarrollo de la política de seguridad de impresión y soluciones de seguridad de las redes de Sharp



SCT – Sharp Consulting Team, **SRDM** – Sharp Remote Device Manager, **DSK** – Data Security Kit, **MFP** – Multifunction Printer, **JAII** – Job Accounting II, **CPO** – Cloud Portal Office

Conclusión

¿Qué hemos aprendido? La buena noticia es que no todo son malas noticias

Si bien las impresoras estándar y las impresoras multifunción presentan, sin lugar a dudas, una amenaza grave (actualmente subestimada) para las empresas, se pueden adoptar varios pasos claros para reducir el riesgo.

- **No está solo: las amenazas están por todas partes.** Todos los días oímos hablar de empresas de todos los tamaños que sufren violaciones de la seguridad, ciberataques, infecciones de virus y otras actividades maliciosas. Lo más importante es entender cómo se puede ver afectada su empresa si fuera atacada y preguntarse si está realmente preparada para defenderse.

- **La solución no es siempre sencilla.** Entender, configurar y ejecutar las medidas y funciones de seguridad adecuadas puede llevar años y entrañar auténticas dificultades de implementación. Como cada organización es diferente, debe aplicar herramientas distintas e introducir estrategias únicas para abordar las amenazas específicas para su empresa. Sin embargo, sean cuales sean sus necesidades particulares, Sharp puede ayudarle a crear una solución efectiva de seguridad para proteger sus impresoras estándar e impresoras multifunción.

- **Si su empresa no está prepara, intente entender el problema.** ¿Por qué es vulnerable su empresa? ¿Tiene suficientes herramientas y recursos para introducir y mejorar su política de seguridad de impresión y de red? ¿O debería recurrir a especialistas de Sharp para auditar sus redes y periféricos conectados, e introducir herramientas de seguridad adecuadas para su empresa?

Entorno de seguridad de Sharp

- **Fije sus propios objetivos de seguridad.** Para entender las posibles vulnerabilidades a las que se enfrenta y qué necesita proteger, debe responder a estas preguntas: «¿dónde se encontrará mi organización en el plazo de unos años?» y «¿cómo puedo preparar mi empresa a fin de dar los pasos necesarios para introducir las medidas y las herramientas adecuadas con el objetivo de impedir ciberataques, malware, etc. en el futuro?»

- **Asegúrese de que cuenta con la competencia adecuada.** Si cuenta con los recursos internos adecuados, puede desarrollar su propia política de seguridad de impresión. O puede recurrir al equipo de servicios profesionales de Sharp para que le ayuden a desarrollar un sistema de seguridad efectivo y a introducir las herramientas adecuadas para su tipo de empresa y necesidades, incluidos:

  - Dispositivos de red seguros de Sharp, compatibles con los últimos certificados de seguridad
  - Software, soluciones y servicios de seguridad de Sharp que pueden ayudarle a desarrollar una política de seguridad de

impresión: DSK, SRDM, auditoría de seguridad de impresión, etc.

- **Estamos aquí para ayudarle.** Podemos asegurarnos de que no sufra retrasos inesperados en la revisión e implementación de su política de seguridad de impresión. Tiene a su disposición representantes de Sharp para ayudarle a entender el nivel de seguridad actual de su empresa, a revisarlo y a proponerle una estrategia que ofrecerá una política de seguridad de impresión adecuada a las necesidades y los requisitos de su organización. Nuestros especialistas le ayudarán a seleccionar las herramientas y los servicios pertinentes a partir de los siguientes:

  - Funciones estándar de seguridad de Sharp
  - Herramientas opcionales, como SRDM
  - Mejoras opcionales, como DSK
  - Paquete de seguridad de las redes de Sharp
  - Auditoría de seguridad de Sharp
  - Política de seguridad de Sharp.

- **Parta siempre de una visión de conjunto.** Para evitar posibles vulnerabilidades en otras áreas de su organización, podemos ayudarle a introducir medidas de seguridad adicionales desde la cartera de Sharp, para ayudarle a contar protección de seguridad integral en cada aspecto de su empresa.

  - Seguridad de las redes
  - Seguridad de las salidas
  - Seguridad de los documentos
  - Conformidad con el RGPD

Puede obtener más información sobre nuestras soluciones de seguridad en la biblioteca de documentos técnicos o en la sección de seguridad de la información de nuestro sitio web: www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security.htm

También puede ponerse en contacto con su equipo de asesoramiento de soluciones de Sharp.

Referencias

1. Informe «Eastern and Western Europe Single-Function Printer & MFP Market Placements in the last five years», IDC, cuarto trimestre de 2018
2. «IT and Print Security Survey 2015» IDC, septiembre de 2015
3. «Printing: a false sense of security», Quocirca, 2013
4. «Transformative Technology in Document Security», IDC mayo de 2015

`

www.sharp.es

SHARP

Be Original.