# Lista de verificación del cumplimiento en materia de seguridad

## Una práctica lista destinada a proteger los dispositivos de puntos de conexión de red.

Las nuevas normativas están exigiendo a las empresas que se centren más en la seguridad de TI para proteger los datos valiosos de los clientes y de la empresa. Asimismo, directivas como la Reforma General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea, exigen que las empresas evalúen, supervisen y creen informes sobre las brechas de seguridad en cuestión de días.

Con esta continua modificación de las normativas, las empresas están experimentando dificultades para encontrar el tiempo y los recursos necesarios para mantenerse al día. Sin embargo, si únicamente disponen de un simple cortafuegos para protegerse de los ataques, su seguridad podría verse afectada y es posible que tengan que enfrentarse a sanciones que ascienden a millones. Debido a que resulta inevitable que las empresas experimenten una brecha de seguridad en algún momento, es esencial identificar su existencia para corregirla lo antes posible con los productos, procesos y herramientas adecuados.

Esta lista de verificación constituye un práctico recurso para todas aquellas empresas que desean mejorar su seguridad de TI, velar por la reputación de su marca, evitar las costosas consecuencias que supone una brecha y satisfacer las nuevas y estrictas normativas. Comenzando por lo básico, examine la lista hasta los niveles de máxima seguridad y alinee la seguridad de sus puntos de conexión con estas nuevas y estrictas normativas.

# El departamento de TI podrá igualmente utilizar esta práctica lista de verificación para proteger los puntos de conexión de las impresoras.

## Nivel de seguridad básico

- Adquiera únicamente dispositivos con protección malware integrada y unidades de disco duro cifradas.
- Actualice el firmware, especialmente las versiones con revisiones de seguridad críticas (de la misma manera que actualizaría las aplicaciones de su teléfono móvil).
- Configure las interfaces de los dispositivos y bloquee protocolos como FTP y Telnet, que no son necesarios para sus aplicaciones.
- Revise los nuevos dispositivos y cierre los puertos o protocolos que no se estén utilizando actualmente y que podrían servir de punto de acceso a intrusos.
- Utilice contraseñas administrativas únicas para cada dispositivo.
- Bloquee el panel frontal para deshabilitar el acceso a las funciones de administración.
- Cifre los datos que se transmitan al y desde el dispositivo.
- Configure procedimientos de borrado de datos antiguos del disco duro, en especial en el caso de las impresoras que se entreguen.

Una vez haya completado estos pasos, continúe con el siguiente nivel de seguridad.

## Nivel de seguridad medio

- Integre los datos de registro de los sistemas de impresión en su herramienta de gestión de eventos e información de seguridad (SIEM) para supervisar la red de una forma más exhaustiva en caso de que se produzcan amenazas. En lo que respecta a las nuevas normativas de cumplimiento, la visibilidad es primordial cuando se trata de cumplir los requisitos en materia de creación de informes.
- Implemente la autenticación de usuario en la impresora para realizar un seguimiento de quién copia, escanea y envía faxes desde el dispositivo. Estos datos resultan muy útiles en una investigación posterior a una brecha.
- Implemente la impresión pull para evitar que se olvide información confidencial. Esto también contribuye a preservar el medio ambiente, ya que se reduce el número de impresiones desperdiciadas.

Una vez haya completado estos pasos, continúe con el último nivel de seguridad.

## Nivel de seguridad avanzado

- Configure la creación de informes de contabilidad y seguimiento de trabajos.
- Considere la posibilidad de establecer y aplicar automáticamente determinadas normas sobre quién puede acceder y utilizar las impresoras, así como por qué debe realizarse mediante una autorización basada en funciones.
- Implemente certificados digitales únicos para cada impresora, del mismo modo que lo haría con otros dispositivos de la red conectados a Internet.
- Implemente una solución de impresión móvil gestionada para el cifrado de datos, el acceso a los dispositivos de la red, y la autenticación y seguimiento de los usuarios.

4AA7-1093ESE