



Lista de verificación del cumplimiento en materia de seguridad



El reglamento general de protección de datos de la Unión Europea exige la implementación de medidas técnicas y organizativas por parte de las empresas con el fin de proteger la información personal y, potencialmente, notificar a las personas y autoridades afectadas en el caso de una brecha de seguridad que afecte a datos personales.

Esto constituye un desafío para las empresas dado que deben encontrar el tiempo y los recursos necesarios para satisfacer este cumplimiento.

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 las empresas podrían experimentar 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 y evitar las costosas consecuencias que supone una brecha. Comenzando por lo básico, examine la lista hasta los niveles de máxima seguridad para que los puntos de conexión de la impresora se alineen con los requisitos del RGPD.

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



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.