NOTA INFORMATIVA SOBRE MEDIDAS DE SEGURIDAD EN IMPRESORAS

¿Cuál es el problema?

Las impresoras pueden suponer graves problemas para la seguridad de la empresa, incluso las antiguas, Con acceso a la red, pueden tener acceso a datos, servir de entrada y realizar una infección o intrusión.

¿Qué consecuencias puede tener?

Las impresoras pueden ser utilizadas como puerta de entrada al resto de la red desde las que se podrían realizar diferentes ataques como:

- ✓ robo de datos confidenciales, redirigiendo la información que se envía a la impresora a otro lugar;
- ✓ robo de datos confidenciales de los documentos «dejados» en la impresora;
- ✓ escaneo y envío anónimo por correo electrónico de documentos confidenciales;
- ✓ punto de entrada para acceder a la red de la empresa y realizar una infección o intrusión;
- ✓ se pueden utilizar para realizar ataques DDoS a otros equipos o redes.

Estas acciones pueden causar importantes perjuicios económicos y de imagen a nuestra empresa además, el Reglamento europeo de Protección de Datos que entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018, obliga a las empresas a informar de cualquier brecha a la Agencia de Protección de Datos con sanciones por valor del 4% de la facturación.

¿Qué podemos hacer?

Para evitar estas amenazas, debemos incorporar las impresoras en las políticas de ciberseguridad de la empresa, añadiendo **medidas de seguridad específicas** como protegerla con cortafuegos o cifrar las comunicaciones de tal forma que queden controladas y protegidos.

¿Cómo lo hacemos?

Debemos incluirlas en las políticas de seguridad que se aplican a todos los dispositivos y asegurarnos de que el responsable informático aplique las medidas de seguridad como en el resto de dispositivos.
Si se encarga una empresa subcontratada debería garantizar que están configuradas las medidas de seguridad.