Consejos sobre ciberseguridad para pymes

A medida que las empresas dependen cada vez más de las tecnologías de automatización, las probabilidades de sufrir amenazas cibernéticas aumentan. Aunque es probable que las pequeñas y medianas empresas no cuenten con los recursos de las compañías de mayores dimensiones, también deben invertir en infraestructura de seguridad. A continuación ofrecemos tres consejos:

1

Forme a sus empleados

La formación debería incluir los siguientes elementos:

- Cómo utilizar contraseñas fuertes
- Cómo detectar correos electrónicos maliciosos
- Cómo proteger la red wifi doméstica al teletrabajar
- Cómo proteger datos empresariales sensibles o confidenciales
- Cómo detectar e informar de una amenaza cibernética

2

Instale un cortafuegos

Para las pymes, el más adecuado es un cortafuegos de hardware con controles de software, como parte de un sistema de seguridad que incluya soporte de red privada virtual (RPV), antivirus, antispyware y funciones de filtrado de contenidos.

3

Optimice su estrategia en la nube

Escoja plataformas y aplicaciones en la nube que ofrezcan el más alto nivel de seguridad disponible y cuenten con medidas de seguridad integradas para protegerle frente a las vulnerabilidades.

Las consideraciones a tener en cuenta son:

- Accesibilidad, trazabilidad y seguridad
- Escalabilidad: los sistemas de nube han de resultar fáciles de ampliar o reducir para adaptarse a la velocidad a la que crece la empresa.

Una estrategia de nube puede ocuparse de las actualizaciones de datos y la recuperación ante desastres, ofreciendo así una inversión de carácter único sin costes añadidos.

Recuerde que una estrategia de ciberseguridad exitosa es aquella que resulta **proactiva, no reactiva**, lo que significa que las empresas deben invertir en la solución adecuada antes de que suceda algo, en lugar de invertir en respuestas ante lo que suceda.