

Recomendaciones para proteger la seguridad de sus negocios

La migración al mundo digital continúa de forma acelerada en las **pequeñas y medianas empresas (pymes)**. Según el estudio de **Adopción Digital de las Pymes 2022**, elaborado por Telefónica Hispam, la digitalización les genera un **30% de incremento de ventas** y un **27% de ahorro en costos**.

Entre los hallazgos de este sondeo la **ciberseguridad** es una de las **principales preocupaciones** por las vulnerabilidades que puede haber por los ciberataques.

“Las **pymes** son más vulnerables a los ciberataques, ya que muchas no cuentan con un **departamento de TI** dedicado a la seguridad cibernética», precisó el estudio.

Lea también: Ciberseguridad: Cinco claves para evitar robos en internet

Para mitigar este riesgo, es necesario educar al personal sobre buenas prácticas de seguridad, como detectar **phishing** y suplantaciones de identidad, fortalecer el uso de contraseñas seguras y aplicar autenticación **multifactor**.

El Perú es el cuarto país más atacado de la región, con más de **15 000 millones de intentos de ciberataques en 2022**, según el informe de FortiGuard Labs”, explicó el jefe de productos

digitales B2B de Movistar Empresas, Roberto Igei.

Es así que en el marco del **Día Internacional de las Mipymes**, Movistar Empresas ofrece recomendaciones para que los medianos y pequeños negocios resguarden su información y la de sus clientes.

Lea también: Ciberseguridad: Una necesidad urgente para las empresas en 2023

- 1. Implementar medidas de autenticación segura.** Utilizar contraseñas fuertes y cambiarlas regularmente. Además, implementar la autenticación **multifactor**, que combina elementos que el usuario conoce en dispositivos que el usuario posee con procesos biométricos para verificar la identidad. Por ejemplo, para acceder a una aplicación, se puede hacer uso de una contraseña como primer método (algo que se conoce), y como segundo método el uso de un código enviado al teléfono móvil (algo que se posee).
- 2. Actualizar e instalar parches regularmente en los sistemas.** Mantener las aplicaciones y los sistemas operativos actualizados para protegerse contra vulnerabilidades conocidas. Asegurarse de instalar los parches de seguridad y actualizaciones proporcionados por los proveedores de **software y hardware** de confianza.
- 3. Separar el acceso a la red wifi para uso propio y el de tus clientes.** Si en el negocio se brinda servicio de **internet** wifi a los clientes, es clave habilitar una red

wifi para el acceso de los clientes finales. De ese modo se evitará que personas no autorizadas accedan a los recursos de la empresa, sistemas internos o información sensible del negocio. Además, se podrá priorizar el **uso de internet** para el negocio y aplicar medidas de ciberseguridad más estrictas con los empleados.

4. **Proteger los dispositivos y habilitar servicios de ciberseguridad en nube.** Esto significa implementar medidas para una navegación segura en internet, como un firewall virtual o dedicado que habilite la protección hacia y desde internet, además de restringir accesos a sitios web peligrosos. Es importante asegurarse también de que todos los dispositivos utilizados en la empresa, computadoras y dispositivos móviles, estén protegidos con software actualizados de seguridad, así como realizar regularmente análisis en los dispositivos en busca de posibles amenazas.
5. **Capacitar y concienciar al personal.** Brindar capacitación regular sobre buenas prácticas de seguridad, como el reconocimiento de correos electrónicos maliciosos (**phishing**), el uso seguro de contraseñas y la identificación de posibles amenazas. Es importante Fomentar una cultura de seguridad cibernética en toda la organización.
6. **Realizar copias de seguridad de forma regular.** Es importante asegurarse de realizar copias de seguridad de todos los datos importantes y almacenarlos en un lugar seguro, preferiblemente en una ubicación externa o en la nube. Las copias de seguridad periódicas garantizarán que los datos se puedan recuperar en caso de pérdida,

robo o ataque **cibernético**.