Guía práctica: Ciberseguridad para PYMEs

La ciberseguridad es fundamental para proteger la información, los sistemas y la reputación de una empresa. Esta guía ofrece recomendaciones básicas y avanzadas adaptadas a PYMEs.

Principios básicos de la ciberseguridad:

- Confidencialidad: proteger los datos frente a accesos no autorizados.
- Integridad: garantizar que la información no sea alterada sin permiso.
- Disponibilidad: asegurar que los sistemas y datos estén accesibles cuando se necesiten.

Medidas preventivas recomendadas:

- Usar contraseñas seguras y cambiarlas periódicamente.
- Activar la autenticación de dos factores (2FA).
- Mantener actualizados los sistemas operativos y programas.
- Instalar antivirus y firewall actualizados.
- Realizar copias de seguridad automáticas y almacenarlas fuera de la oficina.
- Restringir el acceso a información sensible solo a empleados autorizados.
- Formar al personal en buenas prácticas de seguridad.

Gestión de incidentes de seguridad:

1. Detectar rápidamente la amenaza mediante sistemas de monitorización.
2. Aislar el sistema afectado para evitar la propagación.
3. Notificar al responsable de seguridad o proveedor informático.
4. Aplicar el plan de contingencia y recuperar datos de copias de seguridad.
5. Informar a clientes o proveedores si se ven afectados.

Recomendaciones adicionales para PYMEs:

- Implantar políticas internas claras de seguridad digital.
- Realizar auditorías periódicas de seguridad informática.
- Utilizar redes VPN seguras en teletrabajo.
- Controlar los dispositivos móviles de empresa con sistemas MDM.
- Adoptar soluciones en la nube con certificaciones de seguridad reconocidas.