

¡BLINDA TU NEGOCIO!

7 Hábitos de ciberseguridad para la empresa.

No basta con un antivirus. El 94% de los ataques son por error humano.

1 Gestión de contraseñas y accesos

Complejidad total - Usa claves robustas con caracteres especiales (\$), números (4), mayúsculas y símbolos (!). Prohibido reutilizarlas.

Gestores de contraseñas - Utiliza herramientas como Bitwarden, LastPass o 1Password.

Eficiencia - El equipo solo memoriza una "Contraseña maestra" robusta; el gestor genera y completa automáticamente el resto con claves aleatorias de alta seguridad.

2 Actualización de software y parches de seguridad

Piloto automático - Configura actualizaciones automáticas en Windows y macOS fuera del horario laboral.

Software invisible - Mantén siempre al día lectores de PDF, WinRAR, navegadores y plugins de WordPress.

Fin de soporte - Si usas Windows 10, el soporte ha terminado el 14 de octubre de 2025. Trabajar sin soporte oficial es dejar la puerta abierta a vulnerabilidades.

3 Verificación en Dos Pasos (2FA)

Segunda cerradura - Actívalo en email corporativo, banca online y CRM.

Apps de autenticación - Prioriza Google o Microsoft Authenticator frente al SMS (que es interceptable).

Notificaciones push - Usa sistemas de "un solo toque" vinculados al móvil para confirmar accesos autorizados.

4 Detección de Phishing

Remitente enmascarado - No te fíes del nombre que ves. Revisa siempre la dirección de correo completa.

Verificación directa - Ante la duda, no hagas clic. Contacta con la persona o entidad por otra vía habitual.

5 No uses WiFi público

Riesgo de exposición - En redes de hoteles o aeropuertos, tus contraseñas pueden ser capturadas.

Conexión segura - Comparte datos desde tu smartphone y utiliza siempre una VPN para acceder a recursos de la empresa en la modalidad de teletrabajo.

6 Copias de seguridad (Regla 3-2-1)

El **backup** es tu único seguro de vida contra el **Ransomware** (secuestro de datos).

- **3 Copias:** Los datos originales + 2 respaldos.
- **2 Soportes:** Ej. Un disco duro físico y almacenamiento en la nube.
- **1 Fuera de la empresa:** Una copia debe estar siempre externa o desconectada de la oficina.

7 Cultura de Ciberseguridad

Equipo = Cortafuegos - La tecnología no sirve si el factor humano falla.

Reporte sin miedo - Si un empleado comete un error, debe avisar rápido para contener el ataque. Premia la prudencia, no castigues el fallo accidental.

Formación - Aplica simulacros de phishing y "píldoras de seguridad" de 5 minutos en tus reuniones. La ciberseguridad, en el día a día de tu empresa.

¿Dudas?

Consulta nuestra guía completa en:
cosmomedia.es/blog/ciberseguridad