LO QUE TODA EMPRESA DEBERÍA HACER

Checklist de Ciberseguridad

Pasos concretos que puedes implementar esta semana, sin ser experto en tecnología.

technologies

EMPRESA	RESPONSABLE	FECHA

No necesitas ser experto en tecnología para proteger tu empresa.

Este checklist está pensado para gerentes, directores y dueños de empresas medianas. Cada acción puede completarse en menos de una hora. Marca cada casilla cuando la completes.

1 Accesos y Contraseñas

La causa #1 de brechas en empresas medianas

- [ ] **Activa autenticación de dos pasos (MFA) en el correo corporativo**
  Gmail, Outlook y cualquier servicio en la nube lo tienen gratis en configuración de seguridad.
- [ ] **Cambia todas las contraseñas predeterminadas de routers, cámaras y servidores**
  Si la contraseña es 'admin' o '1234', cualquiera puede entrar. Cámbiala hoy.
- [ ] **Elimina cuentas de empleados que ya no trabajan contigo**
  Cada cuenta activa sin dueño es una puerta abierta para un atacante.
- [ ] **Usa contraseñas únicas por servicio, nunca repitas la misma**
  Considera un gestor de contraseñas como Bitwarden (gratuito) para tu equipo.

2 Correo Electrónico

El 90% de los ataques llegan por correo

- [ ] **Capacita a tu equipo para reconocer correos de phishing**
  Muéstrales ejemplos reales de correos falsos. 30 minutos pueden evitar un desastre.
- [ ] **Activa el filtro anti-spam y anti-phishing en tu servidor de correo**
  Google Workspace y Microsoft 365 ya lo incluyen, solo hay que activarlo.
- [ ] **Nunca abras archivos adjuntos inesperados, aunque vengan de contactos conocidos**
  Si no esperabas ese PDF o Excel, llama al remitente antes de abrirlo.
- [ ] **Verifica que tu dominio tenga SPF, DKIM y DMARC configurados**
  Esto evita que alguien suplante tu correo. Pídele a tu equipo técnico que lo verifique.

3 Respaldo de Datos

Si hoy perdiste todo, ¿podrías recuperarlo mañana?

- [ ] **Haz una copia de seguridad de todos los datos críticos hoy mismo**
  Incluye contratos, bases de datos de clientes, facturas y archivos operativos.

- [ ] **Guarda al menos una copia fuera de la oficina o en la nube**
  Si hay ransomware o incendio, necesitas una copia que no esté en el mismo lugar.

- [ ] **Prueba que puedes restaurar tus respaldos, no basta con hacerlos**
  Un respaldo que nunca se ha probado puede fallar cuando más lo necesitas.

- [ ] **Automatiza los respaldos para que ocurran sin intervención manual**
  Los respaldos manuales se olvidan. Configura una tarea automática diaria o semanal.

4 Dispositivos y Software

Un software desactualizado es una invitación abierta

- [ ] **Actualiza todos los sistemas operativos y aplicaciones esta semana**
  Las actualizaciones cierran vulnerabilidades que los atacantes ya conocen y explotan.

- [ ] **Instala un antivirus actualizado en todos los equipos de la empresa**
  Asegúrate de que esté activo y con las definiciones al día en cada computadora.

- [ ] **Desinstala software que nadie usa**
  Cada programa instalado es un punto de entrada potencial. Si no se usa, se elimina.

- [ ] **Bloquea los equipos automáticamente después de 5 minutos de inactividad**
  Una pantalla desbloqueada en una oficina puede comprometer toda la empresa.

5 Red y Acceso Remoto

Trabaja desde cualquier lugar, pero de forma segura.

- [ ] **Cambia la contraseña del router de la oficina por una fuerte y única**
  La contraseña del router debe cambiarse periódicamente.

- [ ] **Separa la red WiFi de invitados de la red interna de trabajo**
  Clientes y visitas no deben estar en la misma red que tus servidores.

- [ ] **Usa VPN para conectarte a los sistemas de la empresa desde casa o viajes**
  Sin VPN, tu conexión es visible para cualquiera en la misma red pública.

☐ **Bloquea el acceso remoto directo desde internet si no lo necesitas**
El acceso remoto expuesto es uno de los vectores más explotados en LATAM.

¿Cuántas casillas pudiste marcar?

Anota tu puntaje y vuelve a revisar este checklist cada trimestre.

_____ / 20

¿Necesitas ayuda para implementar estos pasos?

Solicita una Evaluación de Seguridad gratuita.

Nuestro equipo revisa tu situación y te da un plan concreto, sin costo.