Checklist de Ciberseguridad para PyMEs

Una guía práctica de auto-evaluación — ConsultasIT

Este checklist le ayuda a evaluar rápidamente el estado de seguridad informática de su empresa. Marque cada punto como **Sí**, **No** o **No sé**. Al final obtendrá una idea clara de sus riesgos más urgentes y qué atender primero.

Tiempo estimado: 10-15 minutos. No requiere conocimientos técnicos.

1. Contraseñas y Acceso

El 80% de las brechas de seguridad en PyMEs empiezan con una contraseña robada o débil. Estos son los fundamentos:

Elemento	Sí / No / No sé
¿Todos los empleados usan contraseñas únicas para cada servicio corporativo?	■ ■ ■
¿Las contraseñas tienen al menos 12 caracteres y mezclan letras, números y símbolos?	■ ■ ■
¿Usan un gestor de contraseñas (Bitwarden, 1Password, LastPass) en lugar de post-its o archivos de Excel?	■ ■ ■
¿Tienen autenticación multifactor (MFA) activa en correo corporativo, Google Workspace, Microsoft 365 y bancos?	■ ■ ■
¿Las cuentas de administrador son diferentes a las cuentas de uso diario?	■ ■ ■
¿Revisan y desactivan cuentas de ex-empleados dentro de las 24 horas de su salida?	■ ■ ■

2. Respaldos y Continuidad

Un ransomware puede cifrar todos sus archivos en minutos. La única defensa confiable son los respaldos bien hechos:

Elemento	Sí / No / No sé
¿Tienen respaldos automáticos diarios de servidores y archivos críticos?	■ ■ ■

¿Los respaldos se guardan en una ubicación DIFERENTE al servidor principal (offsite o nube)?	■ ■ ■
¿Al menos una copia de respaldo es inmutable o está desconectada (air-gapped)?	■ ■ ■
¿Prueban la restauración de respaldos al menos una vez por trimestre?	■ ■ ■
¿Sabrían cuánto tiempo tomaría restaurar sus datos después de un incidente (RTO)?	■ ■ ■
¿Saben cuánta información podrían perder en el peor caso (RPO)?	■ ■ ■

3. Protección de Endpoints

Cada laptop y cada celular corporativo es una puerta potencial. Los controles básicos deben estar en TODOS los dispositivos:

Elemento	Sí / No / No sé
¿Todos los equipos (laptops, desktops) tienen antivirus moderno instalado y actualizado?	■ ■ ■
¿El sistema operativo se actualiza automáticamente y dentro de 14 días de publicación del parche?	■ ■ ■
¿Los discos de las laptops están cifrados (BitLocker, FileVault, LUKS)?	■ ■ ■
¿Los teléfonos corporativos tienen bloqueo con PIN/huella y cifrado activado?	■ ■ ■
¿Los empleados saben que no deben instalar software sin autorización?	■ ■ ■
¿Tienen un proceso para borrado remoto de laptops/teléfonos extraviados?	■ ■ ■

4. Correo y Phishing

El correo electrónico es el vector de ataque #1. Más del 90% de los incidentes empiezan con un email malicioso:

Elemento	Sí / No / No sé
¿Tienen un filtro antispam/antiphishing avanzado (más que el básico de Gmail/Outlook)?	■ ■ ■
¿Han hecho capacitación sobre phishing al personal en los últimos 12 meses?	■ ■ ■
¿Saben reconocer dominios sospechosos (typosquatting, homógrafos)?	■ ■ ■
¿Tienen un proceso claro para reportar emails sospechosos antes de hacer clic?	■ ■ ■
¿Las transferencias de dinero tienen verificación por un segundo canal (llamada, WhatsApp)?	■ ■ ■

¿El dominio tiene configurados SPF, DKIM y DMARC correctamente?	■ ■ ■

5. Red y Wi-Fi

La red de su oficina es la puerta de entrada digital. Estos controles básicos reducen el riesgo significativamente:

Elemento	Sí / No / No sé
¿El router de la oficina tiene firmware actualizado?	■ ■ ■
¿Cambiaron la contraseña del admin del router (no está en el valor de fábrica)?	■ ■ ■
¿El Wi-Fi para visitantes está SEPARADO del Wi-Fi corporativo (SSID y VLAN distintas)?	■ ■ ■
¿El Wi-Fi corporativo usa cifrado WPA2-AES o WPA3?	■ ■ ■
¿Los empleados que trabajan remoto usan VPN para conectarse a recursos internos?	■ ■ ■
¿Saben qué dispositivos están conectados a la red corporativa en este momento?	■ ■ ■

6. Respuesta a Incidentes

Un incidente ocurrirá eventualmente. La diferencia entre un susto y un desastre está en la preparación:

Elemento	Sí / No / No sé
¿Tienen un plan documentado de qué hacer ante un incidente de seguridad?	■ ■ ■
¿Todos saben a quién llamar PRIMERO si sospechan de un ataque?	■ ■ ■
¿Tienen identificado cuáles son sus activos digitales más críticos?	■ ■ ■
¿Tienen contratado o identificado un proveedor de respuesta a incidentes?	■ ■ ■
¿Han simulado al menos una vez un escenario de ataque (phishing, ransomware)?	■ ■ ■
¿Saben a qué autoridad reportar en Ecuador en caso de brecha de datos?	■ ■ ■

Cómo interpretar sus resultados

Si tiene 30+ Síes:

Excelente. Su empresa está sustancialmente mejor protegida que el promedio de PyMEs ecuatorianas. Enfoque sus esfuerzos en los Noes específicos y consolide con revisiones semestrales.

Si tiene entre 20 y 29 Síes:

Posición intermedia. Hay bases sólidas pero también gaps importantes. Identifique los 3-5 puntos más críticos de los Noes y agende remediación dentro de los próximos 90 días.

Si tiene menos de 20 Síes:

Riesgo elevado. Múltiples vectores de ataque sin protección adecuada. Recomendamos una auditoría completa y un plan de remediación priorizado. ConsultasIT ofrece este servicio — contáctenos para agendar una revisión.

Si tiene muchos 'No sé':

La incertidumbre en sí misma es un riesgo. Una auditoría técnica resolverá los unknowns y le dará claridad sobre el estado real de su seguridad.

Siguiente paso

Si este checklist reveló gaps que le preocupan, agende una consulta gratuita con ConsultasIT. Revisaremos sus resultados en conjunto y le propondremos un plan de remediación concreto con plazos y costos claros.

Contacto: https://consultasit.com/#contacto