

RECURSO GRATUITO · 2026

Checklist de ciberseguridad para pymes

24 controles en 6 áreas para saber en qué punto está la seguridad de tu empresa y qué corregir primero. Marca, suma tu puntaje y prioriza.

24

controles de seguridad

6

áreas evaluadas

5 min

para completarlo



ANTES DE EMPEZAR

Cómo usar este checklist

Es una guía orientativa basada en buenas prácticas generales. Responde con honestidad y, si puedes, hazlo junto a quien administra tus sistemas.

1

Marca una respuesta por control.

Sí si el control está implementado y funciona; Parcial si existe pero está incompleto; No si no existe o no lo sabes.

2

Suma los puntos de cada área.

Sí vale 2 puntos, Parcial 1 punto y No 0 puntos. Cada área suma como máximo 8 puntos.

3

Calcula tu nivel y prioriza.

Pasa los totales a la hoja de puntaje, identifica las áreas con menos puntos y completa el plan de acción.

CÓMO INTERPRETAR TU PUNTAJE TOTAL (SOBRE 48 PUNTOS)

0–39 %	Riesgo alto	Tu empresa tiene brechas básicas que un atacante puede aprovechar. Conviene priorizarlas cuanto antes.
40–64 %	Base incompleta	Tienes controles importantes, pero hay áreas sin cubrir. Cerrar esas brechas reduce el riesgo de forma notable.
65–84 %	Buen nivel, con brechas	La mayor parte de los controles está en su lugar. Revisa las áreas con menor puntaje para completar la protección.
85–100 %	Nivel sólido	Tu empresa cubre casi todos los controles. Mantenlos al día y válídalos con una revisión externa.

Este checklist no es una auditoría ni certifica el cumplimiento de ninguna norma. Es un punto de partida para conversar con tu equipo o con un especialista.

MARCA TUS RESPUESTAS

01

Accesos e identidades

Quién entra a tus sistemas, con qué credenciales y hasta dónde llega.

- | | | | | |
|---|--|--------------------------------|-------------------------------------|--------------------------------|
| 1 | Usamos autenticación multifactor (MFA) en el correo y en cualquier acceso remoto.
Una contraseña robada no basta para entrar si hay un segundo factor de verificación. | ☐
Sí | ☐
Parcial | ☐
No |
| 2 | Cada persona tiene su propio usuario: no compartimos cuentas ni contraseñas.
Sin usuarios individuales no hay forma de saber quién hizo qué. | ☐
Sí | ☐
Parcial | ☐
No |
| 3 | Los permisos de administrador se limitan a quienes los necesitan y se revisan al menos una vez al año.
Menos cuentas con privilegios reducen lo que un atacante puede tomar. | ☐
Sí | ☐
Parcial | ☐
No |
| 4 | Cuando una persona sale de la empresa, desactivamos sus accesos el mismo día.
Las cuentas de exempleados que siguen activas son una puerta olvidada. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

02

Equipos y servidores

Los computadores, celulares y servidores donde vive la información.

- | | | | | |
|---|--|--------------------------------|-------------------------------------|--------------------------------|
| 5 | Todos los equipos y servidores tienen antivirus o EDR administrado y actualizado.
Un antivirus sin actualizar o sin consola central deja equipos sin protección sin que nadie lo note. | ☐
Sí | ☐
Parcial | ☐
No |
| 6 | Windows y las aplicaciones críticas se actualizan con una rutina definida de parches.
Muchos ataques aprovechan vulnerabilidades que ya tienen parche disponible. | ☐
Sí | ☐
Parcial | ☐
No |
| 7 | Los portátiles y celulares con información de la empresa tienen cifrado y bloqueo de pantalla.
Si se pierde un equipo cifrado, la información no queda expuesta. | ☐
Sí | ☐
Parcial | ☐
No |
| 8 | Tenemos un inventario actualizado de equipos y software, con licencias vigentes.
No se puede proteger lo que no se sabe que existe. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

MARCA TUS RESPUESTAS

03

Red y acceso remoto

La puerta de entrada de tu red y cómo se conectan las personas desde fuera.

- | | | | | |
|----|--|--------------------------------|-------------------------------------|--------------------------------|
| 9 | Un firewall protege la red y sus reglas y actualizaciones se revisan periódicamente.
Un firewall instalado pero sin mantenimiento deja de proteger con el tiempo. | ☐
Sí | ☐
Parcial | ☐
No |
| 10 | El Wi-Fi de visitantes está separado de la red interna de la empresa.
Así un dispositivo ajeno no llega a tus servidores ni a tus carpetas compartidas. | ☐
Sí | ☐
Parcial | ☐
No |
| 11 | Empleados y proveedores acceden de forma remota por VPN u otro mecanismo seguro con MFA.
El acceso remoto sin controles es una de las entradas más usadas por los atacantes. | ☐
Sí | ☐
Parcial | ☐
No |
| 12 | Alguien revisa las alertas y los registros (logs) del firewall y de los sistemas críticos.
Sin monitoreo, un incidente puede pasar semanas sin detectarse. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

04

Copias de seguridad y continuidad

Qué pasa con tu operación si pierdes datos o se caen los sistemas.

- | | | | | |
|----|--|--------------------------------|-------------------------------------|--------------------------------|
| 13 | Las copias de seguridad de la información crítica se hacen de forma automática.
Las copias manuales dependen de que alguien se acuerde de hacerlas. | ☐
Sí | ☐
Parcial | ☐
No |
| 14 | Mantenemos al menos una copia fuera de la red principal (nube o almacenamiento inmutable).
Un ransomware cifra también las copias que están al alcance de la red. | ☐
Sí | ☐
Parcial | ☐
No |
| 15 | Probamos restaurar una copia al menos una vez al año.
Una copia que nunca se ha restaurado es una suposición, no una garantía. | ☐
Sí | ☐
Parcial | ☐
No |
| 16 | Tenemos por escrito qué sistemas son críticos y cuánto tiempo podemos estar sin ellos.
Sin esa definición no hay cómo priorizar la recuperación cuando algo falla. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

MARCA TUS RESPUESTAS

05

Personas y datos

El factor humano y el control de la información sensible.

- | | | | | |
|----|--|--------------------------------|-------------------------------------|--------------------------------|
| 17 | El equipo recibe capacitación o simulacros de phishing al menos una vez al año.
Muchos incidentes empiezan con un correo falso que alguien abre. | ☐
Sí | ☐
Parcial | ☐
No |
| 18 | Existe una política de uso de equipos, correo y contraseñas que todos conocen.
Las reglas que no están escritas ni comunicadas no se pueden exigir. | ☐
Sí | ☐
Parcial | ☐
No |
| 19 | Sabemos dónde están los datos personales y sensibles y quién puede acceder a ellos.
Es el punto de partida para protegerlos y para responder ante la Ley 1581. | ☐
Sí | ☐
Parcial | ☐
No |
| 20 | Controlamos la salida de información sensible por USB, correo o nube.
La mayoría de las fugas son errores internos, no ataques externos. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

06

Respuesta, soporte y cumplimiento

Cómo reaccionas cuando algo sale mal y qué respaldo tienes.

- | | | | | |
|----|---|--------------------------------|-------------------------------------|--------------------------------|
| 21 | Hay un procedimiento claro para reportar un incidente y todos saben a quién llamar.
En un incidente, cada hora sin una respuesta ordenada aumenta el daño. | ☐
Sí | ☐
Parcial | ☐
No |
| 22 | Contamos con soporte TI o de seguridad con tiempos de respuesta definidos.
Un tiempo de respuesta acordado evita depender de la buena voluntad de alguien. | ☐
Sí | ☐
Parcial | ☐
No |
| 23 | Después de un incidente revisamos qué falló y corregimos la causa.
Sin esa revisión, el mismo problema se repite. | ☐
Sí | ☐
Parcial | ☐
No |
| 24 | Tenemos política de tratamiento de datos personales y autorización de los titulares (Ley 1581 de 2012).
Es una obligación legal para las empresas que manejan datos personales en Colombia. | ☐
Sí | ☐
Parcial | ☐
No |

Puntos del área: _____ / 8

RESULTADOS

Hoja de puntaje

ÁREA	PUNTOS	MÁXIMO	%
01 Accesos e identidades		8	
02 Equipos y servidores		8	
03 Red y acceso remoto		8	
04 Copias de seguridad y continuidad		8	
05 Personas y datos		8	
06 Respuesta, soporte y cumplimiento		8	
Total		48	

% del área = puntos ÷ 8 × 100. % total = puntos ÷ 48 × 100. Mi nivel: _____

Plan de acción

Empieza por las áreas con menos puntos y por los controles que marcaste como No.

ESTA SEMANA

ESTE MES

ESTE TRIMESTRE

SIGUIENTE PASO

¿Quieres que revisemos tu resultado contigo?

Un consultor de Berruit revisa tu infraestructura, tus accesos, tus copias de seguridad y tu soporte, y te dice qué mejorar primero. El diagnóstico inicial no tiene costo.

✓ Diagnóstico gratuito ✓ Sin compromiso ✓ Respuesta de un consultor real

WEB

berruit.com

WHATSAPP

+57 302 635 4867

TELÉFONO

601 351 9483
+57 314 215 0291

CORREO

info@berruit.com