



HOPPER TECH

ESTUDIO DIGITAL

CONTINUIDAD PYME

Checklist de ciberseguridad para PyMEs

30 controles prioritarios para cuentas, equipos, datos, respaldos, proveedores y respuesta a incidentes.

QUE INCLUYE

30 CONTROLES | 6 FRENTES

Esta lista no certifica seguridad ni cumplimiento legal. Registra conforme, pendiente o no aplica justificado, con evidencia y responsable. Prioriza según riesgo y define la frecuencia de revisión; no esperes al calendario ante cambios o incidentes.

USO LIBRE | DESCARGA DIRECTA | SIN REGISTRO

Material educativo. Adapta cada control al contexto y riesgo de tu organización.

Revisión editorial: 2026-09-08



INVENTARIO Y RESPONSABLES

Los frentes son una organización editorial de Hopper Tech, no una evaluación completa del NIST CSF. [1]

- ☐ 01 Inventariar correo, nube, facturación, dominios, equipos y datos críticos.
- ☐ 02 Asignar una persona responsable por cada activo crítico.
- ☐ 03 Clasificar impacto sobre confidencialidad, integridad y disponibilidad.
- ☐ 04 Identificar qué interrupciones detendrían ventas, cobros o atención.
- ☐ 05 Registrar proveedores, propósito, contacto y fecha de revisión.

IDENTIDAD Y ACCESO

- ☐ 01 Planificar cuentas individuales: inventariar las compartidas y migrar dependencias antes de retirarlas.
- ☐ 02 Activar MFA donde esté disponible; priorizar opciones resistentes a phishing y probar recuperación sin exponer códigos. [2]
- ☐ 03 Reservar privilegios administrativos para tareas administrativas.
- ☐ 04 Usar un gestor de contraseñas y evitar reutilización.
- ☐ 05 Revisar accesos al cambiar funciones o terminar una relación; documentar revocación y traspaso de activos con el responsable.

EQUIPOS Y RED

- ☐ 01 Mantener sistema operativo, navegador y aplicaciones soportados.
- ☐ 02 Programar actualizaciones y revisar fallos; validar compatibilidad y recuperación de los activos críticos. [1]
- ☐ 03 Cifrar dispositivos con información sensible.
- ☐ 04 Configurar bloqueo automático y protección antimalware vigente.
- ☐ 05 Separar red de invitados y cambiar credenciales predeterminadas.



DATOS Y RESPALDOS

- ☐ 01 Recolectar sólo datos necesarios y definir su responsable.
- ☐ 02 Limitar acceso según rol; acordar una cadencia por riesgo y revisar ante cambios de personas, proveedores o datos.
- ☐ 03 Mantener una copia aislada o protegida contra alteraciones del sistema original; definir alcance y frecuencia según necesidad de recuperación. [3]
- ☐ 04 Proteger respaldos contra modificación o borrado no autorizado.
- ☐ 05 Ejecutar una restauración de prueba en entorno aislado, sin sobrescribir producción; registrar integridad, tiempo y datos recuperados. [3]

CORREO Y PROVEEDORES

- ☐ 01 Verificar por un canal independiente conocido los cambios de pago o cuenta bancaria; no usar el contacto del mensaje sospechoso. [4]
- ☐ 02 Capacitar para reconocer phishing, urgencia y adjuntos inesperados.
- ☐ 03 No entregar contraseñas ni códigos MFA por correo o mensajería.
- ☐ 04 Exigir acceso mínimo y fecha de término a proveedores.
- ☐ 05 Definir exportación, soporte y recuperación antes de contratar SaaS.

RESPUESTA Y APRENDIZAJE

- ☐ 01 Definir canal de incidentes y responsable autorizado; revisar alertas y registros para detectar desviaciones, no sólo esperar reportes. [1, 5]
- ☐ 02 Mantener contactos de emergencia accesibles fuera del sistema afectado.
- ☐ 03 Separar contención, recuperación, comunicación y registro según el plan; validar ayuda especializada y obligaciones aplicables. [5]
- ☐ 04 Evitar borrar evidencia por impulso; documentar tiempos y decisiones.
- ☐ 05 Ejercitar el plan con frecuencia acordada según riesgo y tras cambios relevantes; verificar acciones correctivas. [5]



FUENTES Y REFERENCIAS

[1] NIST - CSF 2.0 para pequeñas empresas:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>

[2] NIST - MFA y resistencia a phishing:

<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication>

[3] CIS - Recuperación y pruebas, controles 11.1-11.5:

<https://cas.docs.cisecurity.org/en/latest/source/Controls11/>

[4] NIST - Phishing: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>

[5] NIST - Respuesta a incidentes SP 800-61r3:

<https://csrc.nist.gov/pubs/sp/800/61/r3/final>