LA FIRMA DIGITAL

CIBERSEGURIDAD PARA PYMES

10 prácticas para empezar

Recomendaciones para una conversación entre dirección y TI. No son un ranking de ataques en Colombia ni una auditoría técnica.

01 Conozca su operación

Liste servicios críticos, responsables y dependencias. Empiece por los que detienen ventas o atención.

Compruebe: Inventario revisado con el dueño del proceso.

02 Proteja los accesos

Active MFA donde esté disponible, empezando por administradores y correo. Revise cuentas de emergencia.

Compruebe: Cobertura documentada y excepciones controladas.

03 Reduzca privilegios

Separe tareas administrativas del uso diario. Retire accesos cuando cambien las funciones.

Compruebe: Revisión de una cuenta privilegiada y una baja.

04 Mantenga los sistemas

Priorice parches según exposición y riesgo; pruebe cambios y defina cómo revertirlos.

Compruebe: Registro de actualizaciones y pendientes.

05 Cuide sus datos

Clasifique la información sensible y revise quién puede acceder. Aplique cifrado adecuado.

Compruebe: Revisión de permisos y estado de protección.

10 prácticas para empezar

06 Prepare los respaldos

Aísle las copias del entorno principal. Compruebe recuperación, integridad y permisos.

Compruebe: Restauración de prueba documentada.

07 Observe las señales

Mantenga protección de endpoints y registros útiles. Asigne quién revisa y escala alertas.

Compruebe: Una alerta probada de principio a fin.

08 Entrene al equipo

Explique cómo reportar correos o actividad sospechosa. Practique sin culpabilizar a quien reporte.

Compruebe: Canal conocido y registro de formación.

09 Ensaye la respuesta

Defina contactos, decisiones y comunicaciones. Simule un incidente antes de necesitar el plan.

Compruebe: Acta del ejercicio con acciones y responsables.

10 Revise y mejore

Documente riesgos pendientes y seguimiento. Ajuste prioridades cuando cambien procesos o proveedores.

Compruebe: Plan de mejora con fecha de revisión.

Su próximo paso

Esta guía propone acciones originales de aplicación práctica. NIST CSF 2.0 organiza resultados de gestión de riesgos; CIS IG1 ayuda a priorizar higiene esencial. No existe una selección universal de mejores controles para todas las empresas.

Elija dos acciones según el impacto en su operación, asigne un responsable y una fecha. Use el checklist descargable para registrar evidencias y pendientes.

RTO: tiempo objetivo para recuperar un servicio. RPO: pérdida de datos tolerable expresada en tiempo. Acuérdelos con negocio y contrástelos con pruebas.

Ningún control aislado garantiza que no habrá incidentes. Ajuste el trabajo a su contexto, contratos y capacidad operativa.

Referencias oficiales

NIST CSF 2.0 (2024): funciones y gestión de riesgos
https://doi.org/10.6028/NIST.CSWP.29

NIST SP 1300 (2024): guía de inicio para pymes
https://doi.org/10.6028/NIST.SP.1300

CIS Controls v8.1: referencia de controles
https://www.cisecurity.org/controls/v8-1

CIS IG1: priorización de higiene esencial
https://www.cisecurity.org/controls/implementation-groups/ig1

Recursos y diagnóstico: https://lafirma.digital/#recursos