

Seguridad digital para pequeños negocios

GUÍA INTRODUCTORIA · MATERIAL EDUCATIVO



Protege las cuentas de tu negocio, organiza los accesos y prepárate para responder a incidentes.

Nivel: Principiante · Duración estimada del curso: 3.5–4.5 horas · Precio de catálogo: \$19 USD

Esta guía es una introducción escrita a los temas del catálogo. No equivale a un curso completo ni incluye videos. No otorga certificación oficial ni garantiza empleo.

Tus primeras herramientas

1. Protección de cuentas empresariales

Identifica las cuentas que sostienen tu negocio: correo, cobros, redes sociales y archivos. Protege con contraseñas únicas y MFA. Evita cuentas compartidas y usa roles individuales cuando el servicio lo permita. Confirma cambios de datos de pago por un canal independiente.

2. Gestión de accesos

Aplica privilegios mínimos: cada persona necesita solo los accesos de su función. Revisa permisos al cambiar responsabilidades y revócalos al finalizar una relación laboral. Documenta quién administra cada servicio y cómo recuperar acceso sin depender de una sola persona.

3. Copias de seguridad

La regla 3-2-1 propone tres copias, dos tipos de soporte y una fuera del lugar principal. Incluye una copia aislada o inmutable cuando sea posible. Prueba restauraciones y protege los respaldos con controles de acceso y cifrado adecuados.

De la teoría a tus hábitos

4. Protección de información comercial

Recopila únicamente los datos necesarios para operar. Limita quién puede ver información comercial y de clientes. Evita enviar documentos sensibles por enlaces públicos. Define tiempos de conservación y consulta los requisitos de protección de datos que apliquen a tu país y actividad.

5. Preparación básica ante incidentes

Prepara una lista de contactos y acciones ante pérdida de equipos, accesos sospechosos o fraude. Si sospechas un incidente, registra lo observado, evita borrar evidencia y consulta soporte profesional. No continúes utilizando un equipo comprometido para operaciones sensibles.

Ejercicio seguro

Diseña una lista de cuentas críticas, sus responsables y contactos de emergencia. Define una prueba de restauración de respaldo usando datos ficticios, sin detener operaciones reales.

Antes de continuar

Realiza actividades únicamente en tus propias cuentas, equipos o entornos expresamente autorizados. No compartas contraseñas, códigos ni información privada. Los ajustes pueden variar según tu dispositivo o proveedor; consulta siempre su documentación oficial.