

EBOOK: *Ciberseguridad para Todos – Cómo proteger tu vida digital*

Introducción

Cada **39 segundos ocurre un ciberataque en el mundo**. Y no, no es exageración. Por eso este ebook busca darte herramientas claras, simples y aplicables para que protejas tu información personal, tus dispositivos y, si trabajas en una empresa, también sus datos más valiosos.

La ciberseguridad no es solo un asunto de expertos: todos somos el **primer eslabón de defensa**. Aquí aprenderás a reconocer riesgos, a sospechar de lo que parece demasiado bueno para ser cierto y a aplicar buenas prácticas digitales en tu vida diaria.

Índice

1. **El valor de la sospecha: tu primera defensa digital**
 2. **Cómo los ciberdelincuentes te perfilan: la ingeniería social**
 3. **Capas de ciberseguridad: dispositivos, redes y nube**
 4. **Amenazas más comunes: phishing, malware y ransomware**
 5. **Manual de buenas prácticas digitales**
 6. **Conclusión y plan de acción personal**
-

Desarrollo por capítulos

Capítulo 1: El valor de la sospecha

La primera defensa es **desconfiar**. Todo link, correo, mensaje o promoción debe pasar por tu filtro de sospecha.

👉 Si publicas dónde viajas, el nombre de tu mascota o tus quejas a un banco, le das a los ciberdelincuentes piezas para armar tu perfil.

Actividad: Haz una lista de 3 publicaciones recientes en tus redes. ¿Alguna revela información sensible (familia, ubicación, banco, rutinas)?

Capítulo 2: Ingeniería social – Cómo te estudian para atacarte

Los ataques no empiezan con un virus: empiezan con tu información pública. Esto se llama **ingeniería social**.

Ejemplo: si publicas que viajarás, alguien podría enviarte un correo falso de aerolínea con un link de “confirmación”.

Actividad: Escribe 3 posibles formas en que un ciberdelincuente podría usar tu información pública en redes para engañarte.

Capítulo 3: Capas de ciberseguridad

- **Redes Wi-Fi:** pon contraseñas fuertes, incluso en casa.
- **Redes públicas:** usa siempre **VPN** para navegar seguro.
- **Nube:** activa doble autenticación en Dropbox, Drive o iCloud.
- **Aplicaciones:** descarga solo de tiendas oficiales (App Store, Play Store, Huawei).

Actividad: Revisa en tu celular: ¿tienes doble autenticación activa en tus cuentas más importantes?

Capítulo 4: Amenazas más comunes

- **Phishing:** correos o mensajes con links falsos que parecen reales.
- **Malware:** apps o archivos que instalan software espía en tus dispositivos.
- **Ransomware:** secuestro de la información (muy común en empresas).

👉 Regla de oro: **si algo parece demasiado bueno para ser verdad (pasajes a \$20), probablemente es un fraude.**

Actividad: Busca en tu correo o SMS 2 mensajes sospechosos. ¿Qué señales (ortografía, remitente extraño, link raro) los delatan?

Capítulo 5: Manual de buenas prácticas digitales

1. Usa **contraseñas fuertes y diferentes**. Apóyate en gestores de contraseñas (Google, Apple, Microsoft).
2. Activa la **verificación en dos pasos** en todas tus apps (WhatsApp, Instagram, Facebook, correo).
3. Desconfía de todo link: **“nada es gratis en internet”**.
4. Mantén tus dispositivos y aplicaciones siempre **actualizados**.
5. Instala un **antivirus** en PC, tablet y celular.

Actividad: Descarga un gestor de contraseñas y guarda al menos 3 claves diferentes en él.

Capítulo 6: Conclusión y plan de acción

La ciberseguridad no es un lujo: es una necesidad. Cada persona es responsable de proteger su identidad digital. Si aplicas estas prácticas, reducirás enormemente el riesgo de ser víctima de fraudes o robos.

Checklist de seguridad personal:

- Mis redes Wi-Fi tienen contraseña segura
 - Activo la doble autenticación en mis cuentas
 - Uso un gestor de contraseñas
 - Descargo apps solo de tiendas oficiales
 - No hago clic en links sospechosos
 - Mantengo mis dispositivos actualizados
-