CIBERSEGURIDAD VENEZUELA

Protege tus Activos Digitales en Venezuela

---

1. Introducción: ¿Por qué importa la ciberseguridad hoy en Venezuela?

En un país donde muchos de nuestros trámites, comunicaciones y pagos se realizan ahora en línea, **la ciberseguridad** deja de ser algo opcional y pasa a ser una necesidad diaria. Desde el robo de tu saldo móvil hasta la suplantación de tu cuenta de WhatsApp, los ciberdelincuentes buscan aprovecharse de la falta de conocimiento básico para vulnerar tus datos y robar tu dinero.

En Venezuela, las transacciones bancarias por móvil, los grupos de WhatsApp de tu

está diseñada para cualquier persona, independientemente de su nivel técnico, y te enseñará **paso a paso** cómo reforzar tu protección digital sin complicaciones.

Tip Express: Piensa en tu teléfono y tu computador como si fueran tu casa. Mantener la puerta (contraseñas), las ventanas (apps) y el portón (red) bien asegurados evita visitas indeseadas.

---

2. Higiene Digital Básica

¿Qué es higiene digital? Es mantener tus dispositivos (PC, laptop, móvil) limpios de software malicioso y al día con sus actualizaciones.

1. **Actualizaciones automáticas:** Activa en **Windows Update**, **Android/iOS** y en todas tus apps. Cada parche corrige fallas que los atacantes podrían explotar.
2. **Antivirus gratuito:** Instala soluciones reconocidas como Avast Free o Bitdefender Free. Haz un análisis rápido al menos una vez por semana.
3. **Limpieza de archivos y apps:** Desinstala programas que no uses y borra fotos/videos viejos. Menos “basura” reduce riesgos y acelera tu dispositivo.

Mini-paso rápido: Programa recordatorios en el calendario del móvil para “Actualizar y escanear” cada lunes.

---

3. Contraseñas Seguras y Autenticación Multifactor

Las contraseñas débiles son la puerta principal de entrada de un atacante.

- **Reglas para una contraseña robusta**
    - Mínimo 12 caracteres.
    - Mezcla mayúsculas, minúsculas, números y símbolos.
    - Evita palabras del diccionario o tu nombre.
- **Gestor de contraseñas:** Usa **Bitwarden (gratuito)** o **LastPass Free**, que generan y recuerdan claves por ti. Solo necesitas **una contraseña maestra** fuerte.
- **Autenticación multifactor (MFA):**
    - Actívala en todas tus cuentas clave (email, banca, redes).
    - Usa apps como **Google Authenticator** o **Authy**. Evita los SMS, pues pueden secuestrarte el SIM.

Tip Express: Crea un patrón mnemotécnico: “MiCasa2025#Segura” es mejor que “123456”.

---

4. Detecta y Evita Phishing y Estafas Online

Los ataques de phishing buscan engañarte para que reveles datos o instales malware.

- **Señales de alerta**
    1. **URLs extrañas:** coloca el cursor sobre el enlace antes de hacer clic.
    2. **Errores de ortografía o traducción pobre** en el mensaje.
    3. **Urgencia falsa:** “¡Tu cuenta será cerrada en 5 minutos!”
- **Cómo reaccionar**
    1. No hagas clic.
    2. Borra el correo o chat.
    3. Si crees que es real, ve directamente al sitio oficial (no uses el enlace recibido).

Mini-paso rápido: Instala la extensión **“Netcraft Anti-Phishing”** en Chrome/Firefox.

---

5. Protege tu Red en Casa y el Wi-Fi Público

Tu router es el guardián de tu red doméstica; el Wi-Fi público, un lugar de riesgo.

1. **Router seguro**
    - Cambia la contraseña de fábrica y el nombre (SSID).
    - Activa **WPA2 o WPA3**.
    - Desactiva WPS (“botón mágico”) si no lo usas.
2. **Wi-Fi público**
    - Nunca ingreses datos sensibles (banca, contraseñas) en redes abiertas.
    - Utiliza una **VPN gratuita o económica** (ProtonVPN’s plan gratis o TunnelBear).

Tip Express: Apaga el Wi-Fi del móvil cuando no lo necesites; reduce tu exposición.

6. Seguridad en Redes Sociales y Apps de Mensajería

Compartir es parte de nuestra vida, pero el exceso de información abre puertas.

- **Privacidad en Facebook/Instagram**
    - Configura el perfil como **privado**.
    - Revisa cada mes los permisos de aplicaciones conectadas.
- **WhatsApp/Telegram**
    - Ajusta “Verificado en dos pasos” (PIN de 6 dígitos).
    - Activa “Solo mis contactos” para foto de perfil y última conexión.

Mini-paso rápido: Revisa en WhatsApp → Ajustes → Cuenta → Privacidad cada 15 días.

---

7. Seguridad Móvil: Protege tu Smartphone

Tu celular almacena contraseñas, fotos y chats; protégelo como tu banco.

1. **Bloqueo de pantalla:** usar PIN, patrón o huella.
2. **Permisos de apps:** revisa qué apps acceden a cámara, micrófono y ubicación. Desactiva los que no tengan sentido.
3. **Copias de seguridad:** usa Google Drive (Android) o iCloud (iOS) para guardar tus contactos y fotos cifrados.

Tip Express: Si descargas un APK de terceros, hazlo solo de fuentes confiables (APKMirror).

---

8. Qué Hacer en Caso de Incidente

Si crees que has sido atacado, actúa rápido:

1. **Aisla el dispositivo:** apágalo o quita la conexión a Internet.
2. **Cambia contraseñas críticas:** email, bancos y redes sociales.
3. **Escanea con antivirus:** en otro equipo, descarga un USB booteable de Bitdefender Rescue.
4. **Reporta el incidente:** a tu banco, proveedor de teléfono o a los canales de CONATEL o los cuerpos de seguridad local.
5. **Busca ayuda profesional:** si es un ataque grave (ransomware, robo de identidad), acude a un servicio de ciber-forense.

---

9. Recursos y Herramientas Gratuitas

Herramienta	Descripción	Enlace
Bitwarden	Gestor de contraseñas libre y multiplataforma	https://bitwarden.com
ProtonVPN (plan gratuito)	VPN sin límite de datos en servidor básico	https://protonvpn.com
Malwarebytes Free	Escáner de malware para Windows y Android	https://malwarebytes.com
Have I Been Pwned	Comprueba si tu email fue filtrado	https://haveibeenpwned.com
Google Authenticator	Generador de códigos MFA	Google Play / App Store
CONATEL / Denuncias	Canales oficiales para reportar delitos TI	https://conatel.gob.ve

Tip Express: Guarda este PDF en tu dispositivo y consúltalo cada vez que temas un posible ataque.