GUARDIANA
DIGITAL

Taller online · 30 minutos

México sin sustos digitales

Tarjetas, cajeros, wifi y VPN: cómo pagar con más seguridad y proteger tus datos cuando estás de viaje.

Para mujeres que viajan a México y sus familias

- Guion del taller
- Casos prácticos
- Protocolo si hay fraude
- Checklist de viaje

Elizabeth Ledesma · Guardiana Digital

1 · AGENDA

30 minutos para viajar con un plan

Objetivo: disfrutar del viaje sin paranoia, tomando decisiones sencillas antes de pagar, conectarte a una red o escribir tus datos.

00–03	**Arranque: vacaciones sí, sustos no** Identificar los riesgos más comunes al viajar.
03–09	**Tarjetas, cajeros y terminales** Reducir el riesgo de clonación, robo y fraude.
09–15	**Wifi público, datos móviles y VPN** Entender qué protege una VPN y qué no.
15–21	**Situaciones: ¿qué harías?** Practicar decisiones de viaje seguras.
21–26	**Si pierdo la tarjeta o veo un cargo raro** Actuar rápido y guardar pruebas.
26–30	**Checklist antes de salir** Preparar un plan sencillo.

APERTURA SUGERIDA · 0–3 MIN

«Estamos de vacaciones: queremos playa, tacos y fotos bonitas. No queremos volver con un souvenir sorpresa en la cuenta bancaria. Hoy veremos cómo pagar con cabeza y conectarnos con más seguridad. La idea no es desconfiar de todo: es ponerle cinturón de seguridad a nuestra vida digital.»

Idea clave: ninguna medida es infalible. Combina hábitos seguros, alertas del banco, límites de gasto y reacción rápida.

Cómo reducir el riesgo de clonación

La clonación (o *skimming*) ocurre cuando alguien copia los datos de tu tarjeta con un dispositivo o una terminal manipulada. También hay fraudes por robo, páginas falsas, llamadas engañosas y cargos no autorizados. El chip y el pago sin contacto reducen algunos riesgos frente a la banda magnética, pero no los eliminan todos.

Antes de viajar

- ✓ Pregunta a tu banco qué ofrece: congelar la tarjeta, límites por operación, alertas al instante, tarjetas virtuales y bloqueo desde la app.
- ✓ Lleva dos medios de pago guardados en sitios distintos. No lleves todas las tarjetas y el efectivo juntos.
- ✓ Activa las alertas de cada compra y comprueba que puedes entrar en la app del banco desde el extranjero.
- ✓ Revisa la fecha de caducidad, el PIN y cómo reportar una tarjeta perdida. Nunca apuntes el PIN junto a la tarjeta.
- ✓ Para comprar en internet, usa una tarjeta virtual o un número temporal si tu banco lo ofrece, y no guardes la tarjeta en webs que no necesitas.

Consejo: antes de salir, localiza en la app de tu banco dónde se congela la tarjeta. En un susto, cada minuto cuenta.

Al pagar en tiendas, restaurantes y hoteles

- Mira la terminal: si está rota, parece manipulada o se la quieren llevar fuera de tu vista, pide otra o paga de otra forma.
- Inserta el chip o paga sin contacto. Evita deslizar la banda magnética si hay otra opción.
- No dejes que tu tarjeta desaparezca detrás de la barra. Acompaña la operación o pide que acerquen la terminal.
- Comprueba el importe en la pantalla antes de pagar y revisa el recibo y la notificación.
- Cubre el teclado con la otra mano y no digas el PIN en voz alta ni aceptes «ayuda» para escribirlo.

Si algo no cuadra (terminal rota, prisas, «la máquina no funciona, déjeme la tarjeta»), paga en efectivo o con otra tarjeta. No tienes que dar explicaciones.

Cajeros automáticos

- Elige cajeros dentro de una sucursal bancaria o en lugares bien iluminados y con gente.
- Antes de meter la tarjeta, mira si el lector o el teclado parecen añadidos o se mueven. No fuerces nada: si sospechas, cancela y busca otro cajero.
- Cubre el teclado al escribir el PIN y no aceptes ayuda de desconocidos.
- Si el cajero se queda tu tarjeta o muestra un error raro, no llames al «número de asistencia» que te den ni al que esté pegado en la máquina. Usa el teléfono oficial de tu banco.
- Si hay un error, revisa en la app si se hizo el cargo antes de volver a intentarlo.
- Desconfía de piezas flojas, ranuras extrañas, cámaras añadidas o instrucciones poco habituales. Si algo no cuadra, no lo uses.

«Si el cajero parece que se ha puesto un disfraz, no hace falta investigar: cambia de cajero.»

No toques ni intentes desmontar un dispositivo sospechoso. Aléjate y avisa al establecimiento o al banco.

No existe una señal infalible para detectar un cajero manipulado. La mejor protección es combinar cajeros de sucursal, alertas del banco y reaccionar rápido ante cualquier cargo raro.

Wifi público, datos móviles y VPN

Una VPN crea un túnel cifrado entre tu teléfono y el servidor de la VPN. Ayuda a proteger lo que envías cuando estás en un wifi público, pero **no convierte una web falsa en verdadera, no evita el phishing, no protege un teléfono infectado y no te hace anónima.**

Banca: datos móviles

Para el banco y pagos, usa tus datos o una red de confianza. En hoteles y cafeterías, confirma el nombre exacto de la red con el personal.

VPN de confianza

Elige un proveedor reconocido, con política de privacidad clara y apps oficiales. Evita VPN gratuitas desconocidas con muchos permisos o publicidad invasiva.

Conoce su límite

La VPN pasa parte de la confianza del wifi al proveedor de la VPN. No impide que una estafa te convenza de dar tus claves.

Sin conexión automática

Evita que el móvil se conecte solo a redes abiertas. Al terminar, desconéctate y olvida la red.

Verifica la web

Abre la app del banco o escribe tú la dirección. El candado cifra la conexión, pero no demuestra que la página sea legítima.

Bluetooth y carga

Apaga el Bluetooth si no lo usas. En puertos USB públicos, usa tu propio cargador de enchufe o un cable solo de carga.

Regla práctica: datos móviles para el banco, una VPN de confianza en el wifi público y comprobar siempre la web. Ninguna VPN sustituye esas comprobaciones.

4 · PRACTICA · 15–21 MIN

Situaciones de viaje: ¿qué harías?

CASO A · EL RESTAURANTE

El camarero se lleva tu tarjeta «a la caja» y vuelve cinco minutos después.

Respuesta recomendada: Pide que el cobro se haga delante de ti con una terminal portátil o paga de otra forma. Revisa el cargo y ten las alertas activadas.

CASO B · EL CAJERO

El cajero se queda tu tarjeta y una persona amable se ofrece a llamar a un número pegado en la máquina.

Respuesta recomendada: No llames a ese número ni aceptes ayuda. Contacta a tu banco desde la app o su número oficial y bloquea la tarjeta si hace falta.

CASO C · EL WIFI

En el aeropuerto ves «FREE AIRPORT WIFI» y «AIRPORT_WIFI_FREE_2». ¿Cuál eliges?

Respuesta recomendada: Pregunta al personal cuál es la red oficial. Para el banco, usa tus datos. Una VPN no arregla una red falsa ni una web de phishing.

CASO D · EL SUPUESTO BANCO

Te llaman por cargos sospechosos y te piden el código SMS «para cancelar la operación».

Respuesta recomendada: Cuelga y llama tú al banco por un canal oficial. Nunca compartas códigos, PIN ni contraseñas.

Si sospechas clonación o ves un cargo que no hiciste

1. **Bloquea o congela la tarjeta** desde la app o llamando al número oficial del banco. Nunca uses teléfonos de mensajes, anuncios o pegatinas del cajero.
2. **Reporta el cargo** al banco y pide abrir una reclamación por operación no autorizada. Pregunta si conviene cancelar la tarjeta y pedir otra.
3. **Protege tu cuenta:** cambia las claves si las compartiste o crees que te las robaron, cierra sesiones y activa la verificación en dos pasos.
4. **Guarda pruebas:** hora, importe, comercio, lugar aproximado, recibos, notificaciones y número de incidencia. No publiques los datos completos de la tarjeta.
5. **Si perdiste el teléfono:** llama a tu operador y al banco, bloquea la SIM y las tarjetas, usa la localización o el borrado remoto y cambia primero la contraseña de tu correo principal.
6. **Denuncia** ante las autoridades locales si corresponde y sigue el procedimiento de tu banco.

Recuperar el dinero no está garantizado: por eso conviene actuar rápido. **Nunca compartas** el número completo de la tarjeta, el CVV, el PIN, códigos SMS ni capturas del banco en un chat.

Checklist de viaje

- [ ] Tengo la app oficial del banco y puedo entrar desde el extranjero.
- [ ] Activé las alertas de cada compra y sé cómo congelar o bloquear la tarjeta.
- [ ] Tengo el teléfono oficial del banco apuntado fuera del móvil.
- [ ] Llevo medios de pago separados y no guardo el PIN junto a la tarjeta.
- [ ] Actualicé el móvil y las apps, con bloqueo de pantalla y localización remota.
- [ ] Sé cuándo usar datos móviles y cómo elegir una VPN de confianza.
- [ ] Desactivé la conexión automática a redes wifi abiertas.
- [ ] Sé qué hacer si pierdo el móvil o la tarjeta, o si veo un cargo desconocido.

«No se trata de viajar mirando por encima del hombro. Se trata de disfrutar con un plan: tarjeta a la vista, PIN protegido, alertas activadas y cabeza fría con el wifi. Que el único cargo inesperado del viaje sea el de los tacos extra.»

Dónde pedir ayuda

CIERRE SUGERIDO

«Una VPN puede ayudar, pero no es una capa mágica de invisibilidad. La mejor protección combina hábitos, tecnología y reacción rápida.»

Tu banco

Contacta siempre desde la app oficial, el número impreso en la tarjeta o la web que escribas tú.

CONDUSEF (México)

condusef.gob.mx — orientación para usuarias de servicios financieros en México.

Emergencias en México

911, línea nacional de emergencias. Para denuncias, usa los canales oficiales del estado donde estés.

Este material es educativo y no sustituye las condiciones, instrucciones ni procedimientos de seguridad de tu banco. Las opciones de bloqueo, tarjetas virtuales y reclamación cambian según el banco y el país.

HERRAMIENTAS QUE RECOMIENDO

Para viajar más tranquila

Estas son dos herramientas que uso y que encajan con lo que hemos visto en el taller.

Surfshark

VPN

Una VPN para proteger tu conexión cuando uses el wifi del hotel, la cafetería o el aeropuerto. Recuerda: ayuda en redes públicas, pero no sustituye usar datos móviles para el banco ni comprobar la web.

Conseguir Surfshark

https://surfshark.club/friend/eUdkJqBy

Revolut

Cuenta y tarjetas

Únete a los más de 80 millones de clientes que ya estamos encantados con Revolut. Desde la app puedes congelar tu tarjeta al momento, recibir una alerta con cada pago y crear tarjetas virtuales para comprar en internet.

Abrir mi cuenta Revolut

https://revolut.com/referral/?referral-code=anaeli_tl_k2sh!NOV1-26-AR-H1&geo-redirect

Transparencia: estos son enlaces de afiliada o de invitación. Si te registras con ellos, Guardiana Digital puede recibir una comisión o un beneficio, sin coste extra para ti. Solo recomiendo herramientas que uso. Lee siempre sus condiciones antes de contratar.

GUARDIANA
DIGITAL

Buen viaje, y sin sustos

Soy Elizabeth Ledesma, profesional de la ciberseguridad especializada en el factor humano. En Guardiana Digital ayudo a mujeres y familias de España y México a proteger su vida digital con calma y sin tecnicismos.

Más talleres y guías

Guía «¿Mamá, soy yo?», talleres para familias, detox digital para adolescentes, IA Silver y formación para pymes.

guardianadigital.es · guardianxdigital@gmail.com

© 2026 Guardiana Digital · Elizabeth Ledesma. Material educativo de uso personal.