CNSD

Centro Nacional
de Seguridad Digital

GUIA PARA COMPRAS SEGURAS POR INTERNET

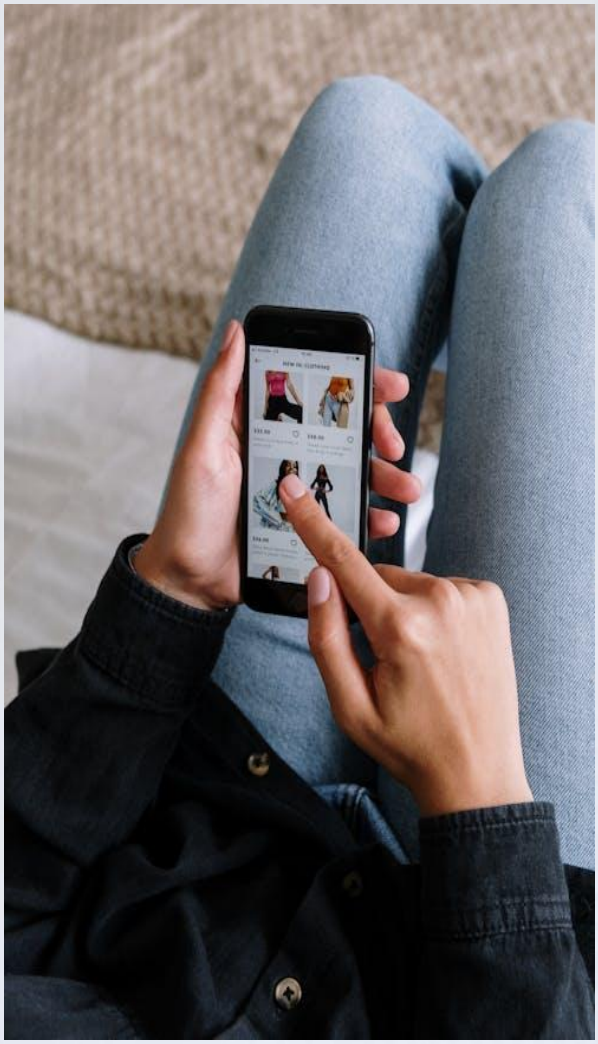
PERÚ | Presidencia del Consejo de Ministros

Ponle PUNCHE y ganamos todos PERÚ

Índice

1. Introducción

1.1. Navegando en el Ecosistema Digital de Compras



El comercio electrónico ha **transformado radicalmente nuestros hábitos de consumo**, ofreciendo una comodidad y una variedad sin precedentes. Desde la comodidad de nuestro hogar, podemos adquirir productos y servicios de cualquier parte del mundo. Sin embargo, esta expansión digital también ha propiciado un aumento en las amenazas cibernéticas, haciendo que la seguridad en las transacciones en línea sea una preocupación primordial.

Esta guía tiene como objetivo proporcionar las herramientas y el conocimiento necesarios para navegar el vasto universo de las compras por internet de manera segura, protegiendo tanto su información personal como financiera.

Abordaremos desde las precauciones básicas hasta las medidas más avanzadas, combinando un lenguaje técnico preciso con explicaciones claras y accesibles.

2. Antes de Realizar una Compra: Preparación y Verificación

La seguridad en línea comienza mucho antes de hacer clic en "comprar". Una preparación adecuada y una verificación exhaustiva son fundamentales para minimizar riesgos.

2.1. Sitios Web de Confianza: El Candado y el Protocolo HTTPS

Antes de introducir cualquier dato personal o bancario, es imperativo verificar la autenticidad y la seguridad del sitio web.

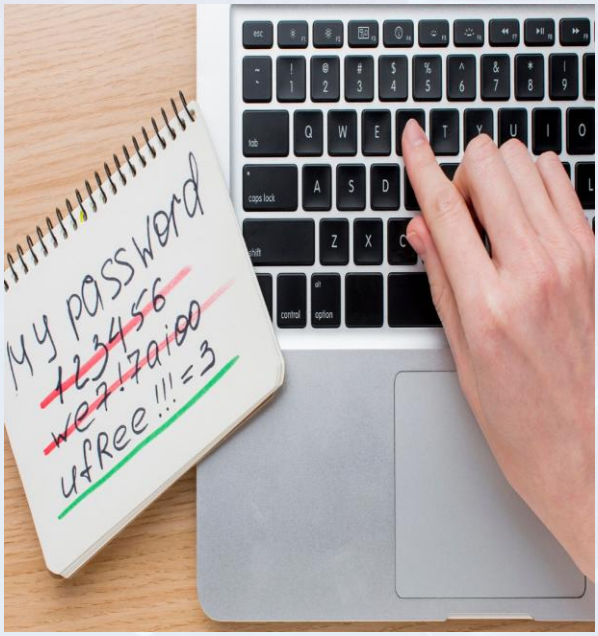
- ✓ **Protocolo HTTPS:** Asegúrese de que la URL del sitio comience con **https://** (Hypertext Transfer Protocol Secure) en lugar de **http://**. La **'S'** indica que la conexión está cifrada, lo que significa que los datos transmitidos entre su navegador y el servidor del sitio web están protegidos contra la interceptación por terceros.

- ✓ **El Candado de Seguridad:** Junto a la URL, debería aparecer un icono de candado cerrado. Al hacer clic en él, podrá ver información sobre el certificado de seguridad del sitio, que verifica la identidad del propietario del dominio. Un certificado válido es una señal de que el sitio es legítimo y que sus datos serán cifrados.
- ✓ **Investigación de Reputación:** Busque reseñas y opiniones de otros usuarios sobre la tienda en línea. Plataformas como Trustpilot, Google Reviews o foros especializados pueden ofrecer una visión valiosa sobre la fiabilidad del vendedor y la calidad de su servicio al cliente. Desconfíe de sitios con pocas o ninguna reseña, o con reseñas excesivamente positivas que parecen falsas.

2.2. Contraseñas Fuertes y Únicas: Su Primera Línea de Defensa

Las contraseñas son la puerta de entrada a sus cuentas. Una contraseña débil es una invitación abierta para los ciberdelincuentes.

- ✓ **Complejidad:** Utilice contraseñas que contengan una combinación de letras mayúsculas y minúsculas, números y símbolos. Evite información personal fácil de adivinar (fechas de nacimiento, nombres de mascotas).
- ✓ **Longitud:** Una contraseña de al menos 12-16 caracteres es ideal. Cuanto más larga, más difícil de descifrar.
- ✓ **Unicidad:** Nunca reutilice la misma contraseña para diferentes cuentas. Si una cuenta se ve comprometida, todas sus otras cuentas que usan la misma contraseña también estarán en riesgo.



Autenticación de Dos Factores (2FA/MFA): Siempre que esté disponible, active la autenticación de dos factores. Esto añade una capa extra de seguridad, requiriendo una segunda verificación (por ejemplo, un código enviado a su teléfono o una huella dactilar) además de su contraseña.

Gestores de Contraseñas: Considere el uso de un gestor de contraseñas (como LastPass, 1Password o Bitwarden). Estas herramientas generan y almacenan contraseñas complejas de forma segura, requiriendo que usted solo recuerde una contraseña maestra.

2.3. Software de Seguridad Actualizado: Antivirus y Firewall

Mantener su sistema operativo y su software de seguridad al día es crucial.

- ✓ **Antivirus y Antimalware:** Un buen programa antivirus detecta y elimina software malicioso que podría intentar robar su información. Asegúrese de que esté siempre activo y que sus definiciones de virus se actualicen regularmente.
- ✓ **Firewall:** Un firewall (cortafuegos) actúa como una barrera entre su red y el internet, controlando el tráfico de entrada y salida y bloqueando accesos no autorizados. Tanto su sistema operativo como su router suelen incluir firewalls.
- ✓ **Actualizaciones del Sistema Operativo y Navegador:** Las actualizaciones de software a menudo incluyen parches de seguridad que corrigen vulnerabilidades conocidas. No posponga estas actualizaciones.

2.4. Evite Redes Wi-Fi Públicas: Un Riesgo Innecesario

Las redes Wi-Fi públicas (en cafeterías, aeropuertos, etc.) son inherentemente inseguras.

Falta de Cifrado: Muchas de estas redes no cifran el tráfico, lo que permite a los atacantes en la misma red interceptar sus datos.

Puntos de Acceso Falsos: Los ciberdelincuentes pueden crear puntos de acceso Wi-Fi falsos para engañar a los usuarios y robar su información.

Recomendación: Evite realizar compras o acceder a información sensible mientras esté conectado a una red Wi-Fi pública. Si es absolutamente necesario, utilice una Red Privada Virtual (VPN) para cifrar su conexión.

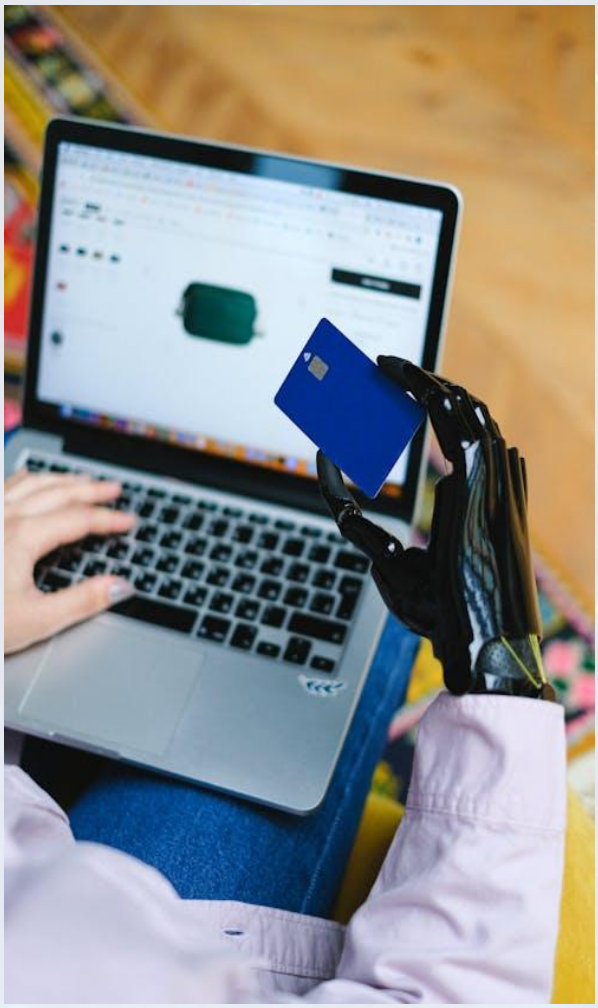
3. Durante la Compra: La Transacción Segura

Una vez que ha verificado el sitio y su entorno es seguro, preste atención a los detalles de la transacción.

3.1. Métodos de Pago Seguros: Priorizando la Protección

La elección del método de pago es vital para su seguridad financiera.

- ✓ **Tarjetas de Crédito:** Son generalmente el método más seguro para compras en línea debido a las protecciones contra el fraude que ofrecen los bancos. En caso de una transacción fraudulenta, es más fácil disputarla y recuperar el dinero.
- ✓ **Plataformas de Pago Seguras (PayPal, Stripe, etc.):** Estas plataformas actúan como intermediarios, lo que significa que usted no comparte directamente los datos de su tarjeta con el comerciante. Ofrecen capas adicionales de seguridad y, a menudo, programas de protección al comprador.
- ✓ **Tarjetas Virtuales o Prepagadas:** Algunos bancos ofrecen tarjetas virtuales de un solo uso o tarjetas prepagadas que puede cargar con la cantidad exacta de su compra, limitando así la exposición de su cuenta principal.



Evite Transferencias Bancarias Directas: A menos que conozca y confíe plenamente en el vendedor, evite realizar transferencias bancarias directas. Una vez que el dinero ha sido transferido, es extremadamente difícil recuperarlo en caso de fraude.

3.2. Verificación de la URL y Phishing: La Amenaza Invisible

El phishing es una de las tácticas más comunes para engañar a los usuarios.

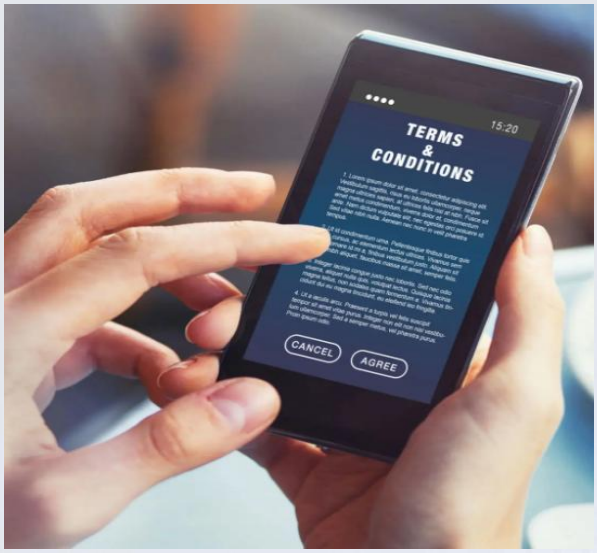
URL Exacta: Antes de introducir sus datos, verifique que la URL del sitio web sea la correcta. Los estafadores a menudo crean sitios web falsos que imitan a los originales, con pequeñas variaciones en la URL (por ejemplo, amaz0n.com en lugar de amazon.com).

Correos Electrónicos y Mensajes Sospechosos: Nunca haga clic en enlaces de correos electrónicos o mensajes de texto sospechosos que le pidan información personal o que le dirijan a un sitio web para "verificar" su cuenta. Siempre acceda al sitio web directamente escribiendo la URL en su navegador.

Errores Gramaticales y Ortográficos: Los sitios de phishing y los correos electrónicos fraudulentos a menudo contienen errores gramaticales u ortográficos evidentes.

3.3. Lea los Términos y Condiciones y la Política de Privacidad

Aunque tedioso, es importante entender las políticas del vendedor.



Política de Devoluciones y Reembolsos: Asegúrese de conocer los términos para devoluciones, cambios y reembolsos. ¿Cuánto tiempo tiene? ¿Quién cubre los gastos de envío?

Política de Privacidad: Entienda cómo el sitio recopilará, usará y protegerá su información personal. ¿Compartirán sus datos con terceros?

Costos Ocultos: Revise si hay cargos adicionales por envío, impuestos o tarifas de procesamiento antes de finalizar la compra.

3.4. Desconfíe de Ofertas Demasiado Buenas para Ser Verdad

Si una oferta parece increíblemente buena, probablemente lo sea.

- ✓ **Precios Irrealmente Bajos:** Los productos con precios significativamente por debajo del promedio del mercado pueden ser falsificaciones, artículos robados o parte de una estafa para obtener sus datos.
- ✓ **Vendedores Desconocidos:** Tenga especial precaución con vendedores que ofrecen precios muy bajos y que no tienen un historial o reputación establecida.

4. Después de la Compra: Seguimiento Post-Transacción

La seguridad no termina con la confirmación del pedido. El seguimiento poscompra es igualmente importante.

4.1. Confirmación del Pedido y Seguimiento

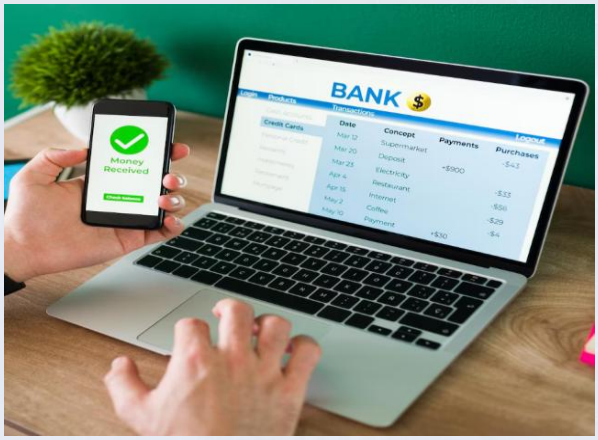
Recibo y Confirmación: Guarde siempre el correo electrónico de confirmación del pedido y cualquier número de seguimiento. Estos documentos son cruciales en caso de disputas o problemas con la entrega.

Monitoreo del Envío: Utilice el número de seguimiento proporcionado para rastrear su paquete. Desconfíe de mensajes que le pidan hacer clic en enlaces para "verificar" el envío si no los ha solicitado.

4.2. Monitoreo de sus Estados de Cuenta Bancarios

Revisión Regular: Revise sus estados de cuenta bancarios y de tarjeta de crédito regularmente (al menos una vez a la semana) para detectar cualquier actividad sospechosa o transacciones no autorizadas.

Alertas Bancarias: Active las alertas de transacciones de su banco para recibir notificaciones por cada compra realizada.



4.3. Política de Devoluciones y Reembolsos

Conozca sus Derechos: Familiarícese con la política de devoluciones del vendedor. Si el producto no es como se describe o llega dañado, saber cómo proceder es clave.

Comunicación: Si surge un problema, comuníquese de inmediato con el servicio al cliente del vendedor. Si no obtiene una respuesta satisfactoria, considere escalar el problema a su banco o a la plataforma de pago.

4.4. Gestión de Correos Electrónicos y Mensajes Sospechosos Post-Compra

Cuidado con el Phishing Dirigido: Los estafadores a menudo envían correos electrónicos de phishing que parecen ser de la tienda donde acaba de comprar, intentando obtener más información o engañarle para que haga clic en enlaces maliciosos.

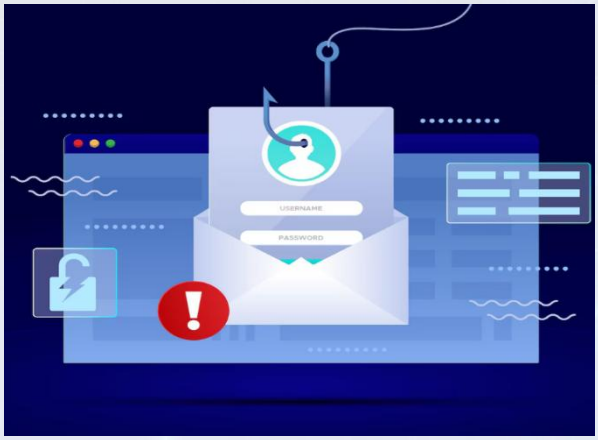
Verifique el Remitente: Siempre verifique la dirección de correo electrónico del remitente. Si parece sospechosa o genérica, es probable que sea un intento de fraude.

5. Amenazas Comunes y Cómo Evitarlas

Comprender las tácticas que utilizan los ciberdelincuentes es fundamental para protegerse.

5.1. Phishing y Spear Phishing

Phishing: Intentos masivos de engañar a los usuarios para que revelen información personal o credenciales a través de correos electrónicos, mensajes o sitios web falsos.



Spear Phishing: Una forma más sofisticada de phishing, dirigida a individuos específicos, utilizando información personalizada para hacer el engaño más convincente.

Prevención: Siempre verifique la URL, el remitente y el contenido de cualquier comunicación sospechosa. No haga clic en enlaces ni descargue archivos adjuntos de fuentes no confiables.

5.2. Malware y Ransomware

Malware: Software malicioso diseñado para dañar o acceder a su sistema sin su consentimiento. Puede ser descargado a través de enlaces engañosos o archivos adjuntos.

Ransomware: Un tipo de malware que cifra sus archivos y exige un rescate (generalmente en criptomonedas) para restaurar el acceso.

Prevención: Mantenga su software antivirus y antimalware actualizado. Sea extremadamente cauteloso con las descargas y los archivos adjuntos. Realice copias de seguridad regulares de sus datos importantes.

5.3. Robo de Identidad

Definición: Ocurre cuando un ciberdelincuente obtiene su información personal (nombre, dirección, número de seguro social, datos bancarios) para cometer fraude en su nombre.

Prevención: Proteja sus contraseñas, no comparta información personal sensible en línea a menos que sea absolutamente necesario y en sitios seguros. Monitoree sus estados de cuenta y su historial crediticio.

5.4. Vulnerabilidades de Wi-Fi Público

Man-in-the-Middle Attacks: En redes Wi-Fi no seguras, un atacante puede interceptar la comunicación entre su dispositivo y el sitio web, leyendo o modificando los datos.

Prevención: Evite transacciones sensibles en Wi-Fi público. Si es inevitable, use una VPN.

5.5. Sitios Web Falsos y Estafas

Sitios Clonados: Replicas exactas de sitios web legítimos, diseñadas para robar sus credenciales o datos de pago.

Estafas de Productos Inexistentes: Vendedores que aceptan pagos por productos que nunca enviarán.

Prevención: Verifique siempre el HTTPS y el candado. Investigue la reputación del vendedor. Desconfíe de precios irrealmente bajos y ofertas por tiempo limitado que presionan a una compra rápida.

6. Protecciones Legales y Qué Hacer si Algo Sale Mal

A pesar de todas las precauciones, los incidentes pueden ocurrir. Saber cómo actuar es crucial.

6.1. Derechos del Consumidor

En Perú, los derechos de los consumidores están protegidos principalmente por el Código de Protección y Defensa del Consumidor, aprobado mediante la Ley N° 29571. Este marco legal establece los principios, derechos y deberes que rigen las relaciones de consumo, incluyendo las transacciones realizadas a través de medios electrónicos.

Algunos aspectos clave de esta legislación que benefician a los consumidores en compras por internet incluyen:

1. **Derecho a la Información:** Los proveedores están obligados a brindar información veraz, clara, completa y oportuna sobre los productos o servicios, incluyendo características, precios, condiciones de venta, garantías y políticas de devolución. En el comercio

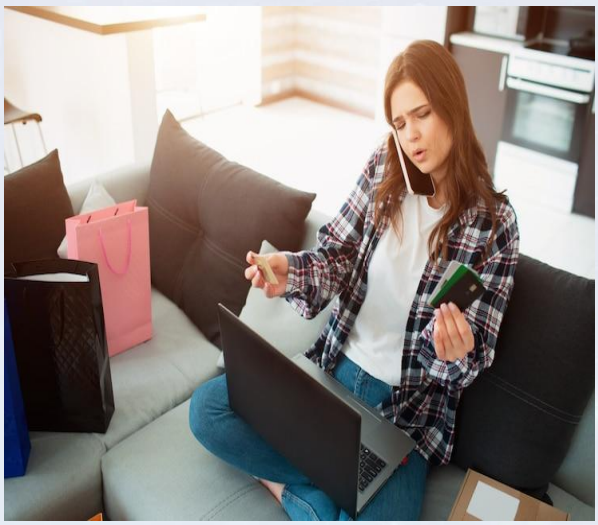
electrónico, esto implica que toda esta información debe estar fácilmente accesible en el sitio web.

2. **Idoneidad del Producto o Servicio:** Los productos y servicios deben ser aptos para los fines que los consumidores esperan de ellos, considerando la información brindada por el proveedor. Si un producto no cumple con lo ofrecido, el consumidor tiene derecho a reclamar.
3. **Garantía:** Los productos y servicios deben contar con las garantías ofrecidas por el proveedor o las establecidas por ley.
4. **Libro de Reclamaciones Virtual:** Los proveedores de comercio electrónico están obligados a contar con un Libro de Reclamaciones virtual, donde los consumidores pueden registrar sus quejas o reclamos. Este debe ser de fácil acceso en el sitio web.
5. **Protección contra Cláusulas Abusivas:** La ley prohíbe las cláusulas abusivas en los contratos, es decir, aquellas que generan un desequilibrio significativo en los derechos y obligaciones de las partes en perjuicio del consumidor.
6. **Protección de Datos Personales:** La Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento, garantizan el derecho fundamental a la protección de la privacidad y el tratamiento adecuado de los datos personales. Los sitios web deben informar sobre el uso que darán a sus datos y obtener su consentimiento.

La institución encargada de velar por el cumplimiento de estos derechos y de resolver controversias entre consumidores y proveedores es el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

6.2. Reportar el Fraude

Contacte a su Banco/Emisor de Tarjeta: Si detecta una transacción fraudulenta, contacte a su banco o al emisor de su tarjeta de crédito de inmediato. Ellos pueden bloquear la tarjeta y disputar el cargo.



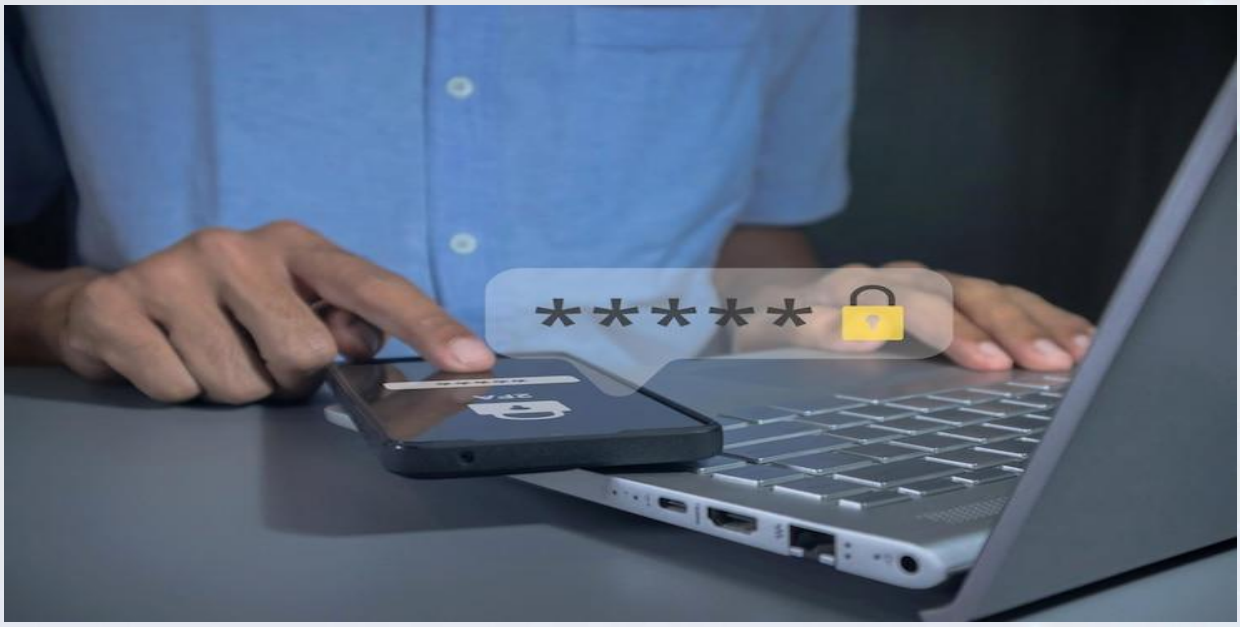
Plataformas de Comercio Electrónico: Si la compra se realizó a través de una plataforma (Amazon, eBay, Mercado Libre), utilice sus mecanismos de protección al comprador y reporte al vendedor.

Autoridades Competentes: Reporte el incidente a las autoridades policiales (Policía Nacional del Perú - División de Investigación de Delitos de Alta Tecnología, DIVINDAT) o a INDECOPI, según corresponda. Esto ayuda a las autoridades a rastrear a los ciberdelincuentes y a prevenir futuros fraudes.

6.3. Recuperación de la Identidad

Alertas de Crédito: Si sospecha de robo de identidad, active alertas de fraude con las agencias de crédito para monitorear cualquier actividad sospechosa en su historial crediticio.

Cambio de Contraseñas: Cambie inmediatamente todas sus contraseñas, especialmente las de sus cuentas bancarias y de correo electrónico.



7. Conclusión: Vigilancia Constante en el Mundo Digital

Las compras seguras por internet no son un evento único, sino un proceso continuo de vigilancia y adaptación. El panorama de las amenazas cibernéticas evoluciona constantemente, y nuestra capacidad para protegernos depende de mantenernos informados y aplicar las mejores prácticas de seguridad.

Al seguir las pautas descritas en esta guía, usted estará mejor equipado para disfrutar de la comodidad y las ventajas del comercio electrónico, minimizando los riesgos y protegiendo su patrimonio digital.

La clave reside en la precaución, la verificación y una respuesta rápida ante cualquier indicio de actividad sospechosa. Compre inteligentemente, compre seguro.

PERÚ | Presidencia del Consejo de Ministros

Ponle PUNCHE y ganamos todos PERÚ

CNSD | Centro Nacional de Seguridad Digital

- alertas@cnsd.gob.pe
- incidentes@cnsd.gob.pe