

GUÍA DE COMERCIO ELECTRÓNICO



ECONOMÍA
SECRETARÍA DE ECONOMÍA

PROFECO
PROCURADURÍA FEDERAL
DEL CONSUMIDOR



INSTITUTO FEDERAL DE
TELECOMUNICACIONES



Si ya eres parte de los usuarios que hacen compras en línea o estás interesado en empezar a realizar compras, esta guía de Comercio Electrónico contiene información importante para que lo hagas de una manera segura.

Los temas que se abordarán son los siguientes:

1. ¿QUÉ ES EL COMERCIO ELECTRÓNICO?
2. PRÁCTICAS PARA UNA COMPRA SEGURA EN INTERNET
3. RIESGOS Y MEDIDAS DE SEGURIDAD



¿QUÉ ES EL COMERCIO ELECTRÓNICO?

Es la compra, venta y comercialización de productos y servicios a través de medios digitales como pueden ser páginas web, a través de las redes sociales, entre otros.¹

Algunos de los tipos de comercio electrónico que existen son²:



- **B2C (Business-to-Consumer):** Estas son las empresas que venden al público en general. Ejemplo: Walmart, Liverpool, Palacio de Hierro, por mencionar algunas.



- **B2B (Business-to-Business):** Son empresas que realizan negocios entre ellas. Un ejemplo son las empresas de logística como FedEx, DHL o Mercado Libre, por mencionar algunas.



- **B2G (Business-to-Government):** Empresas que venden a instituciones de gobierno.



- **C2C (Consumer-to-Consumer):** Plataforma a partir de la cual los consumidores compran y venden entre ellos. En este tipo de comercio podemos localizar los Marketplace de diferentes aplicaciones, como el de Facebook.



¹ Secretaría de economía, disponible en: <https://mipymes.economia.gob.mx/vender/comercio-electronico/#:~:text=El%20comercio%20electr%C3%B3nico%20es%20un,redes%20sociales%2C%20entre%20otros.>

² Visa. ¿Qué es el e-commerce o Comercio electrónico? Disponible en: <https://www.visa.com.mx/dirija-su-negocio/pequenas-medianas-empresas/notas-y-recursos/tecnologia/ques-es-ecommerce-o-comercio-electronico.html>

Ventajas del Comercio Electrónico. Algunas de las más destacadas son³:

- Mejor distribución de los bienes o servicios pues las empresas no requieren de intermediarios, las ventas se realizan a través de sus páginas de Internet. En términos de tiempo resulta una ventaja tanto para las empresas como para los usuarios.
- Se reducen los costos y se elimina la duplicidad de pedidos.
- Fácil acceso para los usuarios, pues estos pueden encontrar ofertas de forma rápida, así como en el caso de las empresas, realizarlas y crear mercados.
- Se mejoran las relaciones entre las empresas y los usuarios, con canales de comunicación más rápidos para conocer más sobre los bienes o servicios.
- La posibilidad de realizar compras las 24 horas del día sin importar donde se encuentre el usuario.



³ Silva Muriillo, Roxana. BENEFICIOS DEL COMERCIO ELECTRÓNICO. PERSPECTIVAS. 2009, Disponible en: <https://www.redalyc.org/articulo.oa?id=425942160008>



PRÁCTICAS PARA UNA COMPRA SEGURA EN INTERNET

Antes de comprar

- Infórmate de la calidad de los productos y la garantía ofrecida por el proveedor.
- Lee las instrucciones de uso publicadas por el proveedor.
- Infórmate de los términos y condiciones aplicables.
- Revisa las políticas de privacidad.
- Conoce tus derechos como consumidor.

Antes de aceptar ofertas, promociones o descuentos, te recomendamos:

- Identificar los productos aplicables.
- Leer los términos y condiciones aplicables.
- Revisar la política de devoluciones o cancelación.

Durante la compra⁴:

- Utilizar una conexión segura a internet.
- Compra en sitios web conocidos y con buena reputación.
- Cerciórate de que estás comprando en el sitio correcto.
- Infórmate sobre los tiempos de entrega.
- Identifica el domicilio del proveedor, números telefónicos o cualquier medio de comunicación para presentar una reclamación.



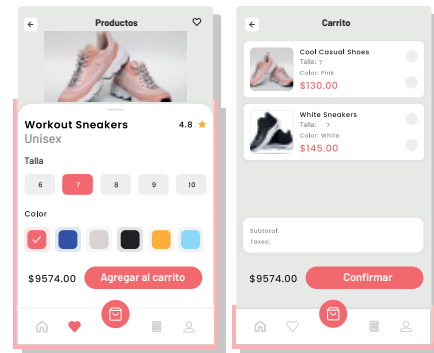
⁴ CONDUSEF, Consejos y Recomendaciones para Comprar en Línea. Disponible en: <https://www.gob.mx/profeco/articulos/consejos-y-recomendaciones-para-comprar-en-linea>

- Cerciórate de que el sitio sea seguro, la URL debe comenzar con https://www. y con un candado al inicio de la URL.
- Establece alertas en tus aplicaciones bancarias y revisa constantemente tus estados bancarios.
- Procura utilizar un solo instrumento de pago en línea.
- Al finalizar tu compra desconéctate y finaliza tu sesión.

Ejemplo.

Proceso de pago

Antes de pagar, revisa el desglose de tu compra y el precio total a pagar. Dentro de la misma página o posterior, observarás un formulario en donde deberás agregar información para contactarte, así como información de la dirección en la que deseas recibir los productos⁵.



⁵ Junta de Castilla y León, Guía del Comercio Electrónico para el Consumidor. Comprar por Internet: fácil, rápido y seguro. Disponible en: <https://bibliotecadigital.jcyl.es/es/consulta/registro.do?id=18564>

Ejemplo.

Una vez que te cercioraste de los productos deseados, el costo total y proporcionaste tu información de contacto, selecciona el método de pago que vas a utilizar para cubrir el total de tu compra, los medios de pago más frecuentes son⁶:

- **Tarjetas de crédito o débito.** Para este método de pago deberás proporcionar datos sobre tu tarjeta como son: Número de tarjeta, fecha de vencimiento y el CVV (3 últimos dígitos en la parte posterior).
- **Transferencia bancaria o depósito.** El proveedor proporciona una cuenta o un número de referencia al que debemos enviar la cantidad total a pagar.
- **A través de terceros** (como Paypal o Mercado Pago). En este método de pago no le proporcionas información sobre tus datos bancarios al vendedor sino a un tercero de confianza que sirve como intermediario.

Ejemplo.

Da "clic" al botón **pagar**, (antes verifica que todo se encuentre en orden). Cuando se ha realizado el cobro se te redirigirá a una página en donde se te informará que el pago ha sido satisfactorio y se te proporcionará un recibo con un número de referencia o de compra (este tiene la misma validez que un ticket de compra en un comercio tradicional), la fecha de entrega y la empresa que realiza el servicio. Esta información también se te proporcionará a través de los medios de contacto que hayas proporcionado, como el correo electrónico.

A través de los medios de contacto que proporcionaste se te hará saber el estado del envío y si existe algún problema con el mismo.

⁶ Idem

Al recibir el producto o servicio.

Una vez finalizada la compra, deberás esperar los días indicados para recibir el producto o servicio solicitado, como pueden ser viajes, reservaciones, boletos de avión, etc.

En caso de no recibir o existir problemas con tu compra, toma evidencias del proceso de compra, el estatus del envío, así como del producto (en caso de que llegara defectuoso) y comunícate con el proveedor para llegar a una solución.

Puedes acercarte a la Procuraduría Federal del Consumidor para hacer valer tus derechos. Recuerda que “todo proveedor está obligado a informar y respetar los precios, tarifas, garantías, cantidades, calidades, medidas, intereses, cargos, términos, plazos y demás condiciones convenidas con el consumidor.”⁷

Devoluciones

El Artículo 53 fracción II, de la Ley Federal de Protección al Consumidor indica que los comercios deben permitir a las personas realizar reclamaciones y devoluciones por medios similares a los utilizados para la venta⁸.

Para solicitar un cambio o devolución:

1. Lo primero que deberás hacer es guardar la información de contacto del vendedor y conservar tus comprobantes de compra.
2. Accede a tu cuenta de la plataforma por la cual realizaste la compra en línea, o contacta con el comercio para realizar el proceso de devolución a través de una solicitud de reembolso o reemplazo del producto o servicio.
3. En ocasiones se te proporcionará un formulario en donde te preguntarán las razones por las cuáles deseas devolver el producto.
4. Posterior a estos pasos se te proporcionará una guía de envío para que puedas enviar tu producto a través de la paquetería seleccionada.
5. Una vez recibido el paquete por el comercio, se te deberá realizar el reembolso del dinero o el cambio del producto.



⁷ Artículo 7 de la Ley Federal de Protección al Consumidor.

⁸ Artículo 53 fracción II, de la Ley Federal de Protección al Consumidor.



RIESGOS Y MEDIDAS DE SEGURIDAD

Dentro del comercio electrónico siempre se espera que las compras estén exentas de problemas, sin embargo, podemos estar expuestos a diversos riesgos presentes en el entorno digital como pueden ser los fraudes cibernéticos. Se le denomina fraude cibernético a aquellas estafas que utilizan la red, para realizar transacciones ilícitas⁹.

Riesgos y fraudes en el comercio electrónico.

Algunos de los principales tipos de fraude que ocurren en el comercio electrónico son los siguientes¹⁰:



- **Spam.** Se trata de un mensaje enviado a varios destinatarios que usualmente no lo solicitaron, con fines publicitarios o comerciales. Te invitan a visitar una página o descargar algún archivo que, por lo general contiene virus que roba información de tu dispositivo.



- **Smishing.** En este tipo de fraude, te envían mensajes SMS a tu teléfono móvil con la finalidad de que visites una página web fraudulenta, con el fin de obtener información bancaria para realizar compras a tu nombre.



- **Phising.** El objetivo de este tipo de fraude es simular ser una institución financiera, indicándote un error en tu cuenta bancaria y te solicitan datos confidenciales como: número de tarjetas de crédito, claves, datos de las cuentas bancarias, contraseñas, etc.



- **Carding.** Hace referencia a "card" que significa tarjeta en inglés, consiste en sustraer datos de las tarjetas de crédito o débito para realizar compras con ellas.



- **Pharming.** Consiste en redirigirte a una página de Internet falsa mediante ventanas emergentes, para robar tu información.



⁹ CONDUSEF, Tipos de Fraude. Disponible en: <https://www.condusef.gob.mx/?p=tipos-de-fraude>

¹⁰ CONDUSEF, Tipos de Fraude. Disponible en: <https://www.condusef.gob.mx/?p=tipos-de-fraude>

Al igual que las tecnologías, los fraudes que se realizan en el comercio electrónico han cambiado y se han adoptado nuevas técnicas para engañar a los usuarios, algunas de esas nuevas técnicas o variaciones de fraudes que utilizan los ciberdelincuentes son:



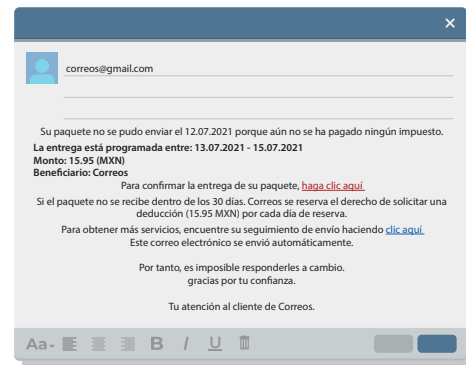
- **Ingeniería social.** Consiste en persuadir y engañar a una persona para influenciarla en sus acciones. Por ejemplo, utilizar la curiosidad de las personas para que abran archivos o ejecuten programas maliciosos, a través de los cuales pueden acceder a información confidencial en los dispositivos, así como credenciales de acceso o controlar de forma remota el dispositivo¹¹.



- **Entrega de paquetes.** En ocasiones podrían llamarte o mandarte un correo en que se incluye un enlace para rastrear un pedido y configurar la entrega de un paquete que no pudo ser entregado. Estos mensajes de primera vista parecen legítimos, pero no debes hacer clic en los enlaces que envían, ni abrir ningún archivo adjunto, pues estos enlaces o archivos pueden contener virus y así los ciberdelincuentes obtienen información confidencial.¹²

Otra variante de estafa se ejecuta de forma que te solicitan marcar a un número y esto puede tener cargos, los avisos de entrega incluyen un número de devolución internacional, lo cual puede suponer altos cargos y tarifas por minutos¹³.

Ejemplo.



¹¹ INCIBE. Ciberseguridad en el comercio electrónico. Disponible en:

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad.pdf

¹² FedEx, Ejemplos de Correos Electrónicos Fraudulentos. Disponible en:

<https://www.fedex.com/es-us/trust-center/report-fraud/fraudulent-email-examples.html>

¹³ FCC. Cómo identificar y evitar las estafas relacionadas con entregas de paquetes. Disponible en: <https://www.fcc.gov/como-identificar-y-evitar-las-estafas-relacionadas-con-entregas-de-paquetes>



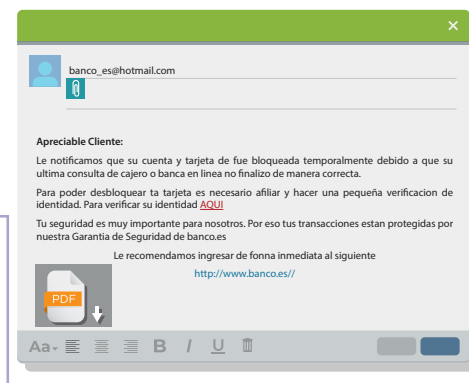
- **Spear Phishing.** Consiste en realizar ataques dirigidos que se enfocan en una sola persona. Por lo general, se realiza a través de correo electrónico utilizando información personal de la víctima para que la misma se encuentre más confiada. Los datos que pueden utilizar los ciberdelincuentes pueden ser información obtenida en redes sociales, blogs personales, información de la basura o cualquier información personal que se pueda encontrar en Internet¹⁴.

Una vez que la víctima descargue el documento PDF adjunto y lo ejecute -lo intente abrir es el modo más habitual, aunque realmente se ejecutan instrucciones introducidas en él-, instala en su equipo un malware con el que el ciberdelincuente podrá ver las credenciales de acceso al gestor de contenido y desde allí, modificar la tienda virtual para así afectar de manera negativa a su imagen corporativa.

Medidas de seguridad

- Instala en tu computadora un buen antivirus.
- No des clic o abras hipervínculos sospechosos.
- Descarga aplicaciones a través de las tiendas y desarrolladores oficiales.
- No proporciones datos personales a través de correo electrónico.
- Si recibes una llamada, recuerda que las empresas y bancos no te solicitan datos financieros, números de tarjetas de crédito.
- Verifica que las páginas de comercio sean conocidas y con buena reputación.
- No respondas mensajes de correo donde te señalan como ganador de un premio, viaje o sorteo.
- Verifica que el sitio web cuenta con el protocolo de seguridad <https://> y un candado en la barra de direcciones.

Ejemplo.



¹⁴ INCIBE. Ciberseguridad en el comercio electrónico. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad.pdf

Referencias

- Instituto Federal de Telecomunicaciones. Ciberseguridad. Disponible en: <https://ciberseguridad.ift.org.mx/>
- CONDUSEF. Tipos de fraude. Disponible en: <https://www.condusef.gob.mx/?p=tipos-de-fraude>
- CONDUSEF. Estadísticas. Disponible en: <https://www.condusef.gob.mx/?p=estadisticas>
- INEGI. ENDUTIH. Disponible en: <https://www.inegi.org.mx/programas/dutih/2022/>
- Procuraduría Federal del Consumidor. Consejos y recomendaciones para comprar en línea. Disponible en: <https://www.gob.mx/profeco/articulos/consejos-y-recomendaciones-para-comprar-en-linea>
- Federal Communications Commission. Disponible en: <https://www.fcc.gov/>
- Federal Trade Commission. Disponible en: <https://www.ftc.gov/>
- INCIBE. Ciberseguridad en el comercio electrónico. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad.pdf
- AMVO. Reporte de Resultados El Buen Fin 2022. Disponible en: <https://www.amvo.org.mx/estudios/reporte-de-resultados-el-buen-fin-2022/>
- Junta de Castilla y León. Guía del Comercio Electrónico para el Consumidor. Disponible en: <https://bibliotecadigital.jcyl.es/es/consulta/registro.do?id=18564>
- FedEx. Ejemplos de Correos Electrónicos Fraudulentos. Disponible en: <https://www.fedex.com/es-us/trust-center/report-fraud/fraudulent-email-examples.html>

