Cámara de Comercio de Bogotá

Pymes ciberseguras

Guía práctica para la prevención de delitos informáticos

En alianza con:

OMNITEMPUS
BEYOND SECURITY

Cámara de Comercio de Bogotá

Ricardo Enrique Nates Escallón
Presidente Ejecutivo (E)

Ana María Fergusson Talero
Vicepresidente de Articulación Público – Privada

Equipo de Trabajo
Dirección de Sostenibilidad, Derechos Humanos y Empresa

José María Balcázar Castillo
Director de Sostenibilidad, Derechos Humanos y Empresa

Natalia Rojas Mateus
Coordinadora de Seguridad, Transparencia y Cultura de la Legalidad

Heydy Marcela Vela Mateus
Profesional Junior Seguridad, Transparencia y Cultura de la Legalidad

Laura Camila Álvarez
Consultora en seguridad

Comité Ejecutivo

Ricardo Nates Escallón
Vicepresidente Ejecutivo (E)

Ana María Fergusson Talero
Vicepresidente Articulación Público - Privada

Constanza Del Pilar Puentes Trujillo
Vicepresidente Servicios Registrales

Karina Galindo Rozo
Vicepresidente Administrativa y Financiera

Leonardo Ortiz
Vicepresidente Jurídica

María del Pilar Londoño Correa
Vicepresidente de Tecnología

María Mónica Conde Barragán
Vicepresidente Relaciones Internacionales

Gustavo Andrés Piedrahita Forero
Vicepresidente Centro de Arbitraje y Conciliación

Juan Carlos González Vergara
Vicepresidente Competitividad

Juan David Castaño Álzate
Vicepresidente Fortalecimiento Empresarial

Darío De La Pava Pulecio
Gerente Recursos Humanos

Carolina Nieto Cáceres
Gerente Asuntos Corporativos

Ángela María Posse Velásquez
Gerente Formación Empresarial

María Elvira Quintana Calderón
Gerente Soluciones y Operación de Eventos

María Paz Gaviria Muñoz
Gerente Plataformas

Natalia Arias Echeverry
Gerente Proyectos Especiales

Carlos Alberto Díaz Rueda
Gerente Planeación e Innovación

Daniel Gómez González
Gerente Articulación Macrosectorial

Andrea González Santos
Contralora

ISBN 978-958-688-533-1
Bogotá, 2023

Omnitempus Ltda.

William Ramírez Castro
Director general

Equipo de Trabajo

Juan Fernando Restrepo Parra
Líder Centro de Análisis de Coyuntura y Seguridad

Giovanni Malaver Kure
Consultor

Juan David Díaz
Consultor

Clover & Clever
Diseño y Diagramación

Pymes ciberseguras

Guía práctica para la prevención de delitos informáticos

Tabla de contenido

¿Sabías que entre 2018 y 2022 incrementó el número de ciberataques en Bogotá en más del 240%?

De no ser así, tal vez sí has oído hablar de casos donde solo con un clic a un correo electrónico o a un enlace de un mensaje de texto, personas y empresas han sufrido robos a sus cuentas bancarias.

Contrario a lo que muchas personas creen, no todos los ataques cibernéticos ocurren a través de virus que se alojan en un computador, los más frecuentes suelen iniciar por una llamada telefónica y terminar incluso con la suplantación de un sitio web. Asimismo, el riesgo de ser víctima de un ciberdelito no existe solo sobre las grandes corporaciones o las entidades del Estado. Las micro, pequeñas y medianas empresas (MIPYMES) son algunos de los principales blancos en la actualidad.

Es por esto por lo que, desde la Cámara de Comercio de Bogotá, en una alianza con Omnitempus, hemos diseñado una guía práctica y concisa que llevará a que tu empresa se convierta en una pyme cibersegura y reduzcas el riesgo de sufrir ataques de esta naturaleza.

¿Qué ventajas tiene ser una pyme cibersegura?

1. Proteges tu información: Implementar medidas de ciberseguridad reduce el riesgo de que tanto tu información como la de tus clientes y proveedores caigan en manos equivocadas.

2. Reduces costos: Al adoptar medidas preventivas, se disminuyen los gastos relacionados con la recuperación de ciberataques y la necesidad de asistencia técnica de emergencia.

3. Cuidas tu reputación: Además de los daños económicos, los ciberataques pueden afectar la buena reputación de tu negocio porque también ponen en riesgo la seguridad de tus clientes.

4. Cumples con las normas: Al cumplir con las regulaciones de seguridad cibernética, como la Ley de Protección de Datos Personales, puedes evitar multas y sanciones, y tener una ventaja competitiva en el mercado.

Ser una pyme cibersegura no requiere de grandes conocimientos informáticos ni tampoco de cuantiosas inversiones en equipos tecnológicos. Únicamente necesitas los dispositivos que normalmente usas, ganas de aprender y seguir paso a paso los consejos de esta guía.

Toma precauciones e incrementa las potencialidades de tu negocio.

¡Conoce!

Conoce los principales tipos de fraude

¿Has recibido correos electrónicos o llamadas telefónicas donde te solicitan con urgencia información personal como número cédula, datos bancarios o claves de tus redes sociales? ¿Recibes mensajes de texto con ofertas demasiado atractivas para ser ciertas o dónde te notifican que ganaste un carro o una millonaria suma de dinero?

Si es así, esto significa que ya has sido una posible víctima de un ataque cibernético. **Los ciberdelincuentes a menudo utilizan la urgencia como una táctica para obtener información confidencial. A diferencia de otros tipos de ciberataques, los más frecuentes se enfocan en explotar las debilidades humanas en lugar de vulnerabilidades técnicas.**

En este primer segmento, te damos señales y ejemplos para que aprendas a detectar cuando estás en riesgo de sufrir alguno de los ataques cibernéticos más comunes hoy en día. Aprenderás a identificar irregularidades que se presenten a través de los canales de comunicación más frecuentes y reducir tus vulnerabilidades.

¿Cómo identificar correos electrónicos maliciosos?

Algunos estudios estiman que el 90% de los ataques cibernéticos inician a través de los correos electrónicos. A través de este canal, ciberdelincuentes buscan obtener información privada de las personas que pueda ser útil con distintos fines, como, por ejemplo, realizar transferencias bancarias de manera ilegítima. **A este tipo de modalidad se le conoce comúnmente como phishing.**

Para determinar la veracidad de un correo, es importante que estés atento a estas señales:

- **Dominio incongruente:** La máxima alerta de un correo electrónico fraudulento se relaciona con el dominio del remitente. Por dominio hablamos del nombre único que se muestra después del signo @ en las direcciones de correo.

Es por esto por lo que lo primero que debes tener en cuenta es en hacer clic sobre la dirección del correo que te llegó y contrastar si su dominio es equivalente con el nombre del remitente.

Por ejemplo, si recibes un correo del Banco Arcoíris que señala que tu cuenta ha sido bloqueada o que verifiques alguna transacción, es fundamental que hagas clic sobre la dirección de remitente y verifiques que después del signo arroba concuerde con el nombre del banco.

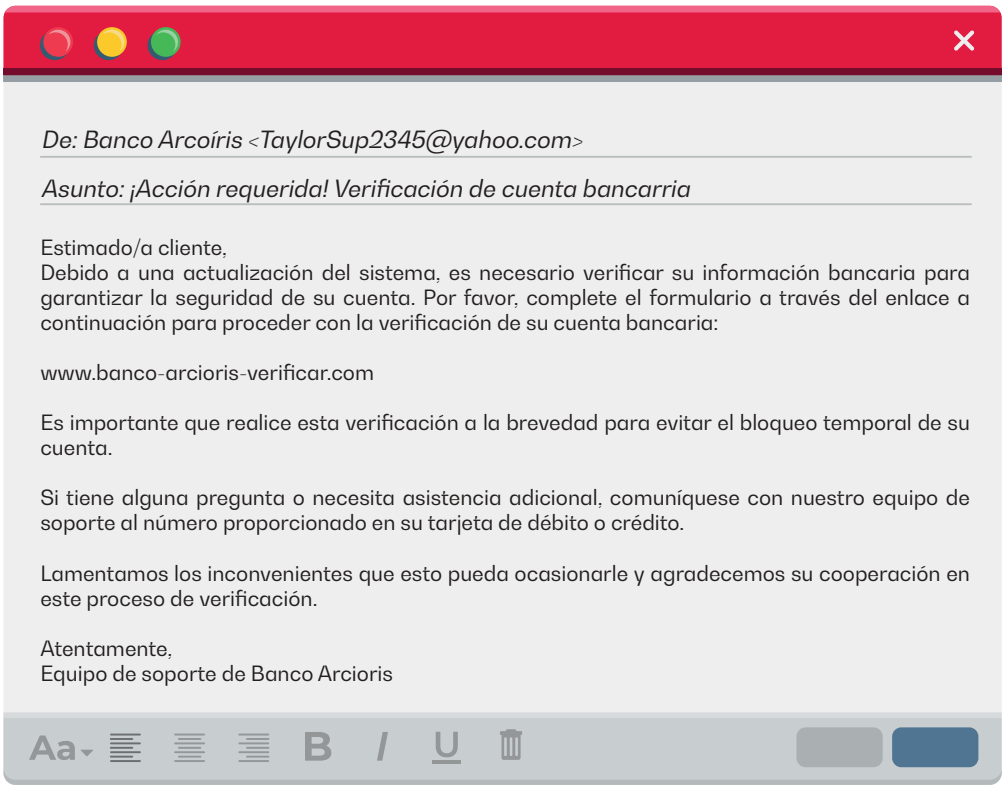
- **Fallas de ortografía y redacción:** Buena parte de los correos tipo *phishing* tienen en común errores garrafales de ortografía y puntuación. Asimismo, muchas veces tienen falta de coherencia entre las ideas que hacen el texto confuso y desconectado.

- **Cuentan con archivos adjuntos:** Desconfía de correos que te inviten a descargar archivos anexos. Esto además implica un factor de doble riesgo, ya que en ocasiones estos archivos pueden incluso alojar un programa espía que extraiga todo tipo de información de tus dispositivos.

Algunas de las narrativas más frecuentes elaboradas por los delincuentes son enviar notificaciones de supuestas foto multas o de alguna incongruencia tributaria de la DIAN a través de corrèo electrónico .

1. Si recibes un correo de la DIAN ten en cuenta que estos contienen un código de verificación que puede ser validado en la dirección web https://muisca.dian.gov.co/WebComunicaciones/DefVerificarCorreoDian.faces

En cualquiera de estos casos, es fundamental que hagas caso omiso, no descargues archivos adjuntos, elimines el correo y bloquees el remitente.



¿Cómo prevenir fraudes por mensaje de texto?

El *smishing* es otra modalidad de ciberdelincuencia que ha incrementado notablemente en los últimos años. Consiste en el envío de mensajes de texto (SMS) de un remitente que simula ser parte de una entidad legítima con el objetivo de hurtar información privada.

Debes tener en cuenta, que los mensajes de texto son mucho más difíciles de detectar que los correos electrónicos de phishing, ya que los filtros de spam no funcionan de la misma manera. Entonces, ¿cómo puedes prevenir ser una víctima de un delito cibernético por mensajes de texto?

- Desconfía de remitentes desconocidos.
- Desconfía de promociones, cupones y/o concursos que prometan demasiado. Son usualmente utilizados como anzuelo para captar la atención de los usuarios.
- No facilites información personal. Entidades gubernamentales o bancarías jamás te solicitarán que verifiques tus datos personales a través de mensajes de texto o WhatsApp.
- No hagas clic en enlaces adjuntos. Los enlaces pueden trasladarte a páginas webs fraudulentas o incluso ejecutar un archivo malicioso que se instale en tu dispositivo y te robe toda la información que digites.

En caso tal que identifiques algunos de estos elementos, te recomendamos eliminar inmediatamente el mensaje y bloquear el número de teléfono del remitente.

¿Cómo identificar llamadas fraudulentas?

¿La ciberdelincuencia también opera a través de llamadas telefónicas? Por supuesto que sí. Esta modalidad es conocida como *vishing.*

De manera similar a las tácticas mencionadas anteriormente, los delincuentes emulan pertenecer a algún tipo de entidad legitima como un banco o una empresa de servicios públicos. ¿Su objetivo? Obtener tus datos confidenciales que puedan ser monetizados de distintas maneras.

Algunas otras señales que podrían indicarte de una llamada tipo *vishing* son:

- La llamada no fue solicitada por ti.
- El número es desconocido.
- Te solicitan información personal como tú número de cédula, códigos que recién te llegaron por mensajes de texto, contraseñas, etc.
- Te solicitan transferencias o pagos urgentes.
- Te presentan ofertas demasiado buenas para ser ciertas.
- Te amenazan si no tomas alguna acción en específico.

En cualquiera de estos casos, **o si tienes dudas sobre la autenticidad de una llamada, es mejor colgar y llamar a la entidad o empresa directamente** utilizando un número de teléfono conocido o que se encuentre en la web oficial.

¿Cómo evitar fraudes en compras en línea?

Imagina que estás buscando un teléfono celular a un precio atractivo en un sitio web de venta en línea. Encuentras un vendedor que ofrece el modelo que deseas a un precio significativamente más bajo que en otras tiendas. Emocionado por la oferta, realizas la compra y realizas el pago en línea. No obstante, después de esperar varios días, el paquete nunca llega. Intentas comunicarte con el vendedor, pero descubres que su número de contacto es falso y el sitio web ha desaparecido. **Te das cuenta de que has sido víctima de una estafa en línea y has perdido tu dinero.**

En la era digital, realizar compras por internet se ha vuelto una práctica común y conveniente. Sin embargo, **con el aumento de la actividad en línea también han surgido riesgos asociados, como los fraudes y estafas electrónicas.**

Te damos algunos consejos para evitar ser una víctima más de estos delitos:

¿Cómo evitar una estafa al vender productos por internet?

Al igual que al comprar, vender en línea también implica un riesgo ya que existen personas malintencionadas que se dedican a estafar a vendedores. Pueden utilizar diversos métodos, como realizar compras con tarjetas de crédito robadas, hacer devoluciones fraudulentas o presentar reclamaciones falsas para obtener reembolsos injustificados.

Ten en cuenta estas cinco recomendaciones para evitar ser víctima de alguna clase de estafa al vender tus productos en la red:

1 Utiliza plataformas y sitios web confiables:

Opta por utilizar plataformas de comercio electrónico reconocidas y sitios web confiables para tus ventas en línea. Estas plataformas suelen contar con medidas de seguridad y políticas de protección al comprador y vendedor.

2 Verifica la reputación del comprador:

Antes de concretar una venta, verifica la reputación del comprador. Revisa los comentarios y calificaciones de otros vendedores que hayan realizado transacciones con esa persona. Si hay señales de alerta o comentarios negativos, considera no seguir adelante con la venta.

3 Utiliza métodos de pago seguros:

Prefiere utilizar métodos de pago seguros, como PayPal u otros servicios similares. Estos servicios brindan protección tanto al comprador como al vendedor en caso de disputas o reclamaciones fraudulentas.

4 Mantén registros detallados de las transacciones:

Guarda un registro completo de todas las transacciones que realices, incluyendo información del comprador, comunicaciones, acuerdos, pruebas de envío y recibos. Esto te será útil en caso de disputas o reclamaciones fraudulentas, ya que contarás con evidencia respaldatoria.

5 Sé cauteloso con las solicitudes de pago inusuales:

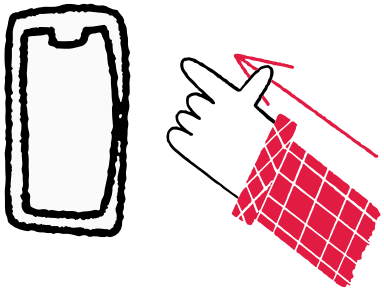
Mantén precaución ante solicitudes de pago que sean inusuales o que te pidan realizar acciones fuera de las plataformas seguras. Evita compartir información financiera confidencial o enviar productos antes de haber recibido el pago adecuado. Si algo parece sospechoso, confía en tu instinto y considera cancelar la transacción.

Píldora ¡Conoce!

Pedro Rodríguez, dueño de una tienda de venta de cosméticos, recibió un correo electrónico en el que se le notifica que ha ganado un premio en efectivo de $10.000.000 por ser un cliente frecuente de una cadena de supermercados. El correo le indica que, para poder reclamar el premio, debe comunicarse con la tienda utilizando un número de teléfono proporcionado.

Pedro no conoce los consejos de esta guía...

1



Pedro decide llamar al número.

2

Un supuesto asesor de la tienda contesta y señala que para poder hacer efectivo el premio, Pedro debe comprar un seguro por el 10% del valor.

3

Para realizar la compra del seguro, Pedro debe hacer una transferencia desde su cuenta bancaria utilizando un enlace enviado por correo electrónico, y proporcionar su información personal.

4

Pedro realiza la transferencia, pero jamás recibe ninguna clase de premio debido a que se trataba de una estafa.

Consecuencias para Pedro...

- Perdió $1.000.000.
- Entregó datos personales que podrían ser mal utilizados por delincuentes en otro tipo de estafas.

Píldora ¡Conoce!

Pedro leyó esta guía y aplica lo aprendido...

- Pedro desconfía porque se trata de un mensaje que promete demasiado.
- Verifica la dirección de correo y nota que el dominio después de la arroba no corresponde con la tienda, sino que se trata de una dirección de Hotmail.
- Pedro nota que el texto del correo tiene fallas de ortografía evidentes.
- Ante la alerta de una estafa, Pedro bloquea el remitente y elimina inmediatamente el mensaje.

Consecuencias para Pedro...

- Evitó ser estafado.

Paso 2

¡Navega!

Navega en internet con seguridad

Ya conoces los principales riesgos y modalidades de ciberdelito en la actualidad, es hora de equiparte con el conocimiento necesario para protegerte mientras exploras la web.

En este apartado, descubrirás una serie consejos que te ayudarán a protegerte de amenazas en línea, preservar tu privacidad y disfrutar de una experiencia segura en internet. Aprenderás cómo conectarte de forma segura a redes Wifi, activar herramientas como el modo incógnito para aumentar la seguridad de tu navegación y cómo detectar páginas web inseguras. Además, recibirás otras recomendaciones importantes de ciberseguridad que te ayudarán a fortalecer tu protección en línea.

¿Cómo conectarnos a internet de forma segura?

Asegúrate de conectarte a redes Wifi seguras y confiables, como las de tu hogar, oficina, redes privadas virtuales (VPN[2] por sus siglas en inglés) o simplemente comparte internet desde tu dispositivo móvil. Evita conectarte a redes Wifi públicas o abiertas que no requieren contraseñas ya que son más vulnerables a ataques cibernéticos.

¿Cómo puedes identificar que una red Wifi es segura?

Al momento que vas a realizar la conexión de uno de tus dispositivos a una red fíjate en estos dos detalles:

- La red Wifi tiene el icono de candado en la parte superior izquierda.

- La red Wifi te solicita una contraseña para poder conectarte.

Las redes Wifi abiertas pueden ser peligrosas debido a su falta de seguridad y cifrado lo que significa que los datos que se transmiten a través de ellas no están protegidos. Los ciberdelincuentes pueden configurar redes Wifi falsas con nombres similares a los de establecimientos populares, como cafeterías o aeropuertos, para engañar a los usuarios y hacer que se conecten a ellas. **A través de estas redes falsas, los atacantes pueden realizar ataques de phishing[3] para robar tus datos personales.**

Asimismo, **en una red Wifi abierta, cualquier persona que esté conectada a la misma red puede potencialmente acceder a tus datos y actividades en línea.** Esto incluye el monitoreo de tus comunicaciones, la visualización de tus archivos compartidos y la interceptación de cualquier dato sensible que envíes o recibas.

Si por algún motivo debes o quieres conectarte a una red abierta, es imprescindible que evites acceder a sitios web que contengan información personal o sensible, como sitios de banca en línea, plataformas de compras o redes sociales. **Asegúrate de tener instaladas las últimas actualizaciones de seguridad en tus dispositivos** ya que estas suelen incluir parches de seguridad que abordan vulnerabilidades conocidas y mejoran la protección contra amenazas.

¿Cómo blindar nuestra conexión a internet?

La seguridad del router de internet es un tema crucial en la protección de nuestras redes y datos. **Como punto de acceso principal a la red, desempeña un papel fundamental en la conectividad y comunicación de los dispositivos.** No obstante, su vulnerabilidad frente a posibles amenazas y ciberataques requiere una atención especial. Es por esto por lo que deberías tener en cuenta estas tres prevenciones con el router de tu oficina y hogar:

2. Es como un túnel privado que protege tu conexión a internet.
3. Se refiere al envío de correos electrónicos que pretenden manipular al receptor para robar información confidencial.

1 Las contraseñas del router se deben cambiar periódicamente.

Para cambiar la clave sigue este paso a paso:

a) Conecta tu computadora al router.

b) Abre un navegador web y escribe la dirección IP del router. Puedes encontrar esta dirección en el manual del router o en línea.

c) Inicia sesión en la configuración del router con el nombre de usuario y la contraseña.

d) Busca la sección de “Configuración de seguridad” o “Configuración inalámbrica”.

e) Cambia la contraseña por una nueva y segura.

f) Guarda los cambios y reinicia el router.

2 Asegúrate de que el software del router esté siempre actualizado con las últimas mejoras de seguridad.

Aunque muchos routers ofrecen actualizaciones automáticas, es importante verificar periódicamente si hay actualizaciones disponibles. Esto lo puedes realizar de la siguiente forma:

a) Abre un navegador web en tu computadora.

b) Escribe la dirección IP del router en la barra de direcciones del navegador y presiona Enter.

c) Inicia sesión en la configuración del router con tu nombre de usuario y contraseña. Suelen estar especificados en el manual del dispositivo o en la documentación proporcionada por el fabricante.

d) Busca una sección que se refiera a las actualizaciones del router.

e) Verifica si hay alguna actualización disponible comparando la versión actual del software del router con la última versión proporcionada por el fabricante.

f) Si la versión actual es más antigua, sigue las instrucciones del fabricante para descargar.

3 Desactiva la función de administración remota

Ya que esto facilita la posibilidad que algún ciberdelincuente acceda al router desde cualquier lugar del mundo. El proveedor de internet debe darte instrucciones de cómo configurar dispositivo pues esas funcionalidades varían con la marca. De lo contrario:

a) Accede a la página de configuración del router. Abre un navegador web e ingresa la dirección IP del router en la barra de direcciones.

b) Inicia sesión en la página de configuración: Ingresa el nombre de usuario y contraseña del router.

c) Encuentra la configuración de administración remota: Navega por las diferentes opciones de configuración hasta encontrar la sección relacionada con la administración remota.

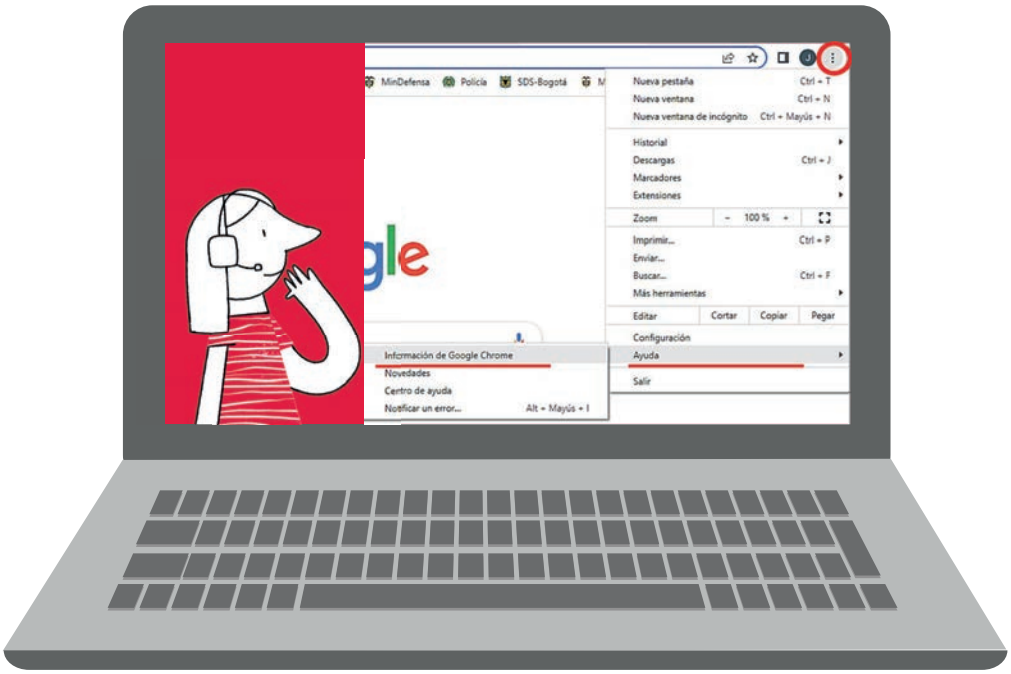
d) Desactiva la función: Una vez que hayas encontrado la opción de administración remota, desactívala.

¿Cómo comprobar que nuestro navegador está actualizado?

Mantener tu navegador web actualizado es esencial para proteger tu información personal, evitar ataques cibernéticos y garantizar una experiencia en línea segura. Las actualizaciones del navegador suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas que podrían ser explotadas por ciberdelincuentes para acceder a tu información personal, instalar programas maliciosos en tu dispositivo o llevar a cabo ataques cibernéticos.

Para comprobar que el software está actualizado, sigue los siguientes pasos dependiendo del navegador que estés utilizando:

Google Chrome	Mozilla Firefox	Microsoft Edge	Safari
1. Haz clic en el menú de tres puntos en la esquina superior derecha de la ventana del navegador. Selecciona “Ayuda” y luego “Acerca de Google Chrome”. 2. La pantalla que aparece te mostrará la versión actual del navegador y si hay actualizaciones disponibles, se descargarán e instalarán automáticamente.	1. Haz clic en el menú de tres líneas en la esquina superior derecha de la ventana del navegador. Selecciona “Ayuda” y luego “Acerca de Firefox”. 2. La pantalla que aparece te mostrará la versión actual del navegador y si hay actualizaciones disponibles, se descargarán e instalarán automáticamente.	1. Haz clic en el menú de tres puntos en la esquina superior derecha de la ventana del navegador. Selecciona “Ayuda y comentarios” y luego “Acerca de Microsoft Edge”. 2. La pantalla que aparece te mostrará la versión actual del navegador y si hay actualizaciones disponibles, se descargarán e instalarán automáticamente.	1. Haz clic en el menú de Apple en la esquina superior izquierda de la pantalla. 2. Selecciona “Preferencias del sistema” y luego “Actualización de software”. Si hay una actualización disponible para Safari, aparecerá en la lista de actualizaciones.



¿Cómo eliminar cookies y el historial de navegación?

Las cookies son pequeños archivos de texto que se almacenan en tu dispositivo cuando visitas un sitio web y que en sí mismas no son necesariamente inseguras. Sin embargo, su uso indebido o **la presencia de cookies maliciosas pueden plantear riesgos para la seguridad y privacidad en línea.**

Para eliminar cookies y el historial de navegación, te presentamos los siguientes pasos dependiendo del navegador que estés utilizando:

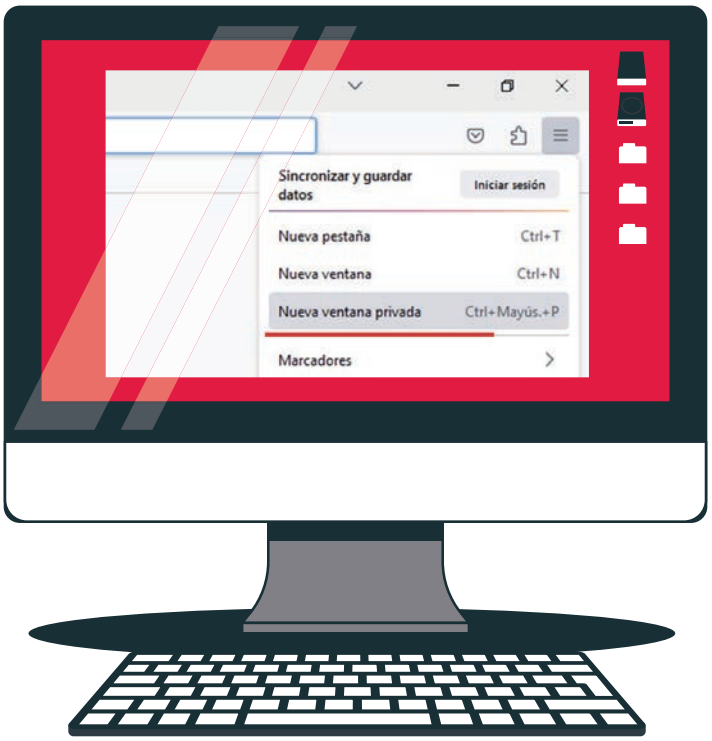
Google Chrome	Mozilla Firefox	Microsoft Edge	Safari
1. Abre el navegador Chrome y haz clic en el icono de tres puntos en la esquina superior derecha de la ventana del navegador. 2. Selecciona “Más herramientas” y luego “Borrar datos de navegación”. 3. Selecciona el rango de tiempo para el que deseas eliminar los datos de navegación y asegúrate de seleccionar “Cookies y otros datos del sitio” y “Historial de navegación”. 4. Haz clic en “Borrar datos”.	1. Abre el navegador Firefox y haz clic en el menú de tres líneas en la esquina superior derecha de la ventana del navegador. 2. Selecciona “Historial” y luego “Borrar historial reciente”. 3. Selecciona el rango de tiempo para el que deseas eliminar los datos de navegación y asegúrate de seleccionar “Cookies” y “Historial”. 4. Haz clic en “Borrar ahora”.	1. Abre el navegador Edge y haz clic en el icono de tres puntos en la esquina superior derecha de la ventana del navegador. 2. Selecciona “Historial” y luego “Borrar datos de navegación”. 3. Selecciona el rango de tiempo para el que deseas eliminar los datos de navegación y asegúrate de seleccionar “Cookies y otros datos del sitio” y “Historial de navegación”. 4. Haz clic en “Borrar ahora”.	1. Abre el navegador Safari y haz clic en “Safari” en la barra de menú en la parte superior de la pantalla. 2. Selecciona “Borrar historial” y luego “Borrar todo el historial”. 3. Para eliminar las cookies, haz clic en “Preferencias” y luego en “Privacidad”. 4. Haz clic en “Administrar datos del sitio web” y luego en “Eliminar todo”.

¿Cómo activar el modo incógnito?

El modo incógnito, o modo privado, es una característica que se encuentra en la mayoría de los navegadores web y que ofrece ciertos beneficios en términos de ciberseguridad. **Al navegar en modo incógnito, se evita que el navegador guarde el historial de navegación, las cookies y los datos de formularios, lo que protege la privacidad.** Además, se crea una sesión aislada que no comparte información con las ventanas regulares del navegador. Esto dificulta el seguimiento en línea y la personalización de anuncios.

A continuación, te explicamos los pasos para activar el modo incógnito en algunos de los navegadores web más utilizados:

Google Chrome	Mozilla Firefox	Microsoft Edge	Safari
1. Abre Google Chrome. 2. Haz clic en el icono de tres puntos en la esquina superior derecha de la ventana del navegador. 3. Selecciona “Nueva ventana de incógnito” o presiona “Control+Mayús+N” en Windows o “Comando+Mayús+N” en Mac.	1. Abre Mozilla Firefox. 2. Haz clic en el menú de tres líneas en la esquina superior derecha de la ventana del navegador. 3. Selecciona “Nueva ventana de navegación privada” o presiona “Control+Mayús+P” en Windows o “Comando+Mayús+P” en Mac.	1. Abre Microsoft Edge. 2. Haz clic en el icono de tres puntos en la esquina superior derecha de la ventana del navegador. 3. Selecciona “Nueva ventana de InPrivate” o presiona “Control+Mayús+N” en Windows.	1. Abre Safari. 2. Haz clic en “Archivo” en la barra de menú en la parte superior de la pantalla. 3. vvSelecciona “Nueva ventana privada” o presiona “Comando+Mayús+N”.

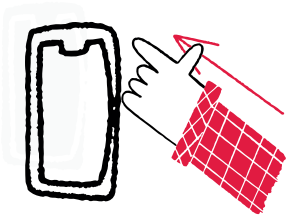


Píldora ¡Navega!

Durante un viaje de trabajo, María, jefa Financiera de la Joyería Damascus, recibe una llamada su jefe solicitándole realizar pagos inmediatos a unos proveedores. Se dirige a la sala de portátiles del hotel donde se hospeda y recibe asistencia del administrador para conectarse a la red Wifi. Tras completar las transferencias, María va a un restaurante del hotel a comer con unos clientes.

María no conoce los consejos de esta guía ...

1



La red Wifi del hotel no le solicitó ninguna contraseña para el ingreso.

2

Busca en Google el nombre del banco y hace clic en el respectivo enlace.

3

Una vez termina, cierra el navegador sin cerrar primero la sesión del portal del banco.

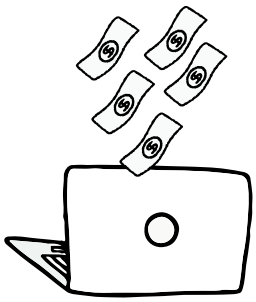
4

El funcionario que la ayudó una vez ella se retira, restaura la sesión del navegador, revisa cookies e historial de navegación y obtiene acceso a la información de María.

5

Finalizando la comida en la que María se encuentra, recibe varios SMS de parte del banco, informándole de transferencias financieras desde la cuenta empresarial no realizadas por ella.

6



María fue víctima de hurto por medios informáticos.

Consecuencias para María

- Es la responsable de la pérdida de dinero de la empresa por malas prácticas en la navegación en internet.
- Los datos de los proveedores caen en manos ajenas.
- Expone a la compañía a posibles multas y sanciones por parte de terceros, contenidas en la ley de protección de datos.

Píldora ¡ Navega!

María leyó esta guía y aplica lo aprendido...

- Se da cuenta que la Wifi a la que le indican conectarse, no le solicita clave.
- Agradece al funcionario la ayuda y le solicita amablemente se retire pues necesita privacidad.
- Comparte el internet de su celular y se conecta con el portátil a la red Wifi propia.
- Ingresa al navegador y activa el modo incógnito y digita la dirección del banco en el navegador.
- Una vez termina el proceso de pagos, cierra la sesión en el portal del banco.
- Cierra el navegador, el cual está utilizando en modo incognito, para que cookies e historial se auto eliminen y desactiva la opción de compartir internet en su celular.

Consecuencias para María

- Pone en práctica las enseñanzas de la guía y verifica que fue una forma segura de hacer movimientos financieros en computadores públicos.
- Comparte a sus funcionarios la experiencia y advierte de las posibles consecuencias de no tener conocimientos básicos para una navegación segura en internet.

Paso 3

¡Protege!

Protege tu información

La información es uno de los activos vitales para cualquier empresa, por lo que su protección debe ser una prioridad fundamental. Ya sea que tu negocio cuente únicamente con un computador o que toda tu operación comercial se lleve a cabo en línea, **todas las empresas poseen datos valiosos que, si caen en manos equivocadas, pueden comprometer tanto la estabilidad económica como la reputación de tu organización.**

En esta sección de la guía, descubriremos prácticas simples pero poderosas que te ayudarán a minimizar el riesgo y la exposición de tu información. Te enseñaremos a implementar medidas de seguridad adecuadas, como establecer políticas de contraseñas fuertes, como activar la verificación en dos pasos en tus plataformas bancarias, correos electrónicos y redes sociales y a crear copias de respaldo y recuperación.

¿Cómo crear contraseñas fuertes?

¿Sabías que una contraseña corta y que solo tenga números o letras puede ser descubierta por un hacker inexperto en cuestión de minutos? Para ser exactos, **algunos estudios estiman que una contraseña compuesta por 5 letras minúsculas puede ser descifrada en tan solo 12 segundos.**

Las contraseñas débiles son fáciles de adivinar o descifrar, ya que generalmente consisten en palabras comunes, secuencias numéricas simples o información personal fácilmente accesible. Es por eso que es crucial utilizar contraseñas seguras y robustas que sean difíciles de adivinar o descifrar.

Ten en cuenta estas recomendaciones a la hora de formular contraseñas, sobre todo, para tus cuentas bancarias, correos electrónicos y redes sociales:

- **Debe ser larga:** Una contraseña segura debe ser lo suficientemente larga. Se recomienda tener al menos 8 caracteres, pero cuanto más extensa sea, mejor. Algunos expertos sugieren utilizar contraseñas de 12 o más caracteres.

- **Mezcla los caracteres:** Es importante combinar diferentes tipos de caracteres, como letras mayúsculas, minúsculas, números y símbolos especiales como !@#$%.

- **Evitar información personal obvia:** No utilices información personal fácilmente disponible, como tu nombre, cumpleaños o nombre de mascotas. Los hackers pueden obtener esa información y usarla para adivinar tu contraseña.

- **No uses palabras comunes:** Evita el uso de palabras comunes o términos del diccionario, ya que estas contraseñas son más fáciles de descifrar utilizando técnicas automatizadas.

- **No reutilices contraseñas:** Utiliza contraseñas únicas para cada cuenta. Reutilizar la misma contraseña en múltiples plataformas aumenta el riesgo de que, si una de ellas se ve comprometida, todas tus cuentas sean vulnerables.

- **Cambia tus contraseñas regularmente:** Es una buena práctica cambiar tus contraseñas cada cierto tiempo, al menos cada tres meses. Esto agrega una capa adicional de seguridad.

¿Sabes cuanto tiempo se demora un hacker en descifrar una clave?

Longitud	Combinación de todos los tipos de caracteres	Sólo letras minúsculas
3 caracteres	0,8 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.265 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2,046 milenios

¿Cómo funciona y cómo activar la verificación en dos pasos?

La verificación en dos pasos, también conocida como autenticación de dos factores es un método de seguridad adicional utilizado para proteger tus cuentas en línea. Además de ingresar tu contraseña, **la verificación en dos pasos requiere un segundo paso de verificación para confirmar tu identidad.**

La verificación en dos pasos aplica para la mayoría de las plataformas y redes sociales que usas diariamente como WhatsApp, Instagram, Facebook, correos electrónicos y portales de banca en línea

El proceso típico de verificación en dos pasos implica lo siguiente:

- **Introducir tu contraseña:** Inicias sesión en tu cuenta utilizando tu nombre de usuario y contraseña como de costumbre.

- **Segundo factor de verificación:** Después de ingresar tu contraseña, se te solicitará un segundo factor de verificación. Esto puede ser algo que solo tú poseas, como un código único generado por una aplicación de autenticación en tu teléfono móvil, un mensaje de texto con un código enviado a tu número de teléfono, entre otros.

- **Verificación exitosa:** Una vez que hayas ingresado el segundo factor de verificación correctamente, se te concederá el acceso a tu cuenta.

La verificación en dos pasos agrega una capa adicional de seguridad porque incluso si alguien descubre o adivina tu contraseña, aún necesitaría acceder al segundo factor de verificación para ingresar a tu cuenta. Esto reduce significativamente el riesgo de que tu cuenta sea comprometida por un atacante.

Aunque activar la verificación en dos pasos puede variar según el servicio en línea que estés utilizando, la ruta general que normalmente debes seguir es:

1. Inicia sesión en tu cuenta en línea y ve a la configuración o seguridad de la cuenta.

2. Busca la opción de "verificación en dos pasos" o "seguridad adicional".

3. Elige el método que deseas usar, como una aplicación en tu teléfono o mensajes de texto.

4. Sigue las instrucciones para configurar el método seleccionado. Puede ser escanear un código QR, ingresar tu número de teléfono o registrar una clave de seguridad física.

5. Configura una opción de respaldo en caso de que no puedas acceder a tu método principal, como códigos de respaldo o información de contacto alternativa.

6. Realiza una verificación de prueba para asegurarte de que todo esté configurado correctamente.

¿Cómo y dónde guardar copias de seguridad de la información?

Realizar copias de seguridad de la información de tu empresa es crucial. Si ocurre un desastre, desde un ciberataque hasta un fallo en el sistema, podrías perder información valiosa y comprometer la continuidad de tu negocio. **Las copias de seguridad te permiten recuperar rápidamente los datos y mantener la operatividad,** evitando interrupciones costosas y protegiendo la reputación de tu empresa.

El proceso para realizar copias de seguridad puede variar dependiendo de los sistemas y herramientas que utilices, pero un paso a paso general que seguro debes tener cuenta es este:

1. Identifica los datos críticos: Determina qué información es esencial para tu negocio y debe ser respaldada. Esto puede incluir archivos importantes, todas las bases de datos que tengan información personal, etc.

2. Selecciona un método de respaldo: Hay varias opciones disponibles, como adquirir un disco duro externo o guardar la información de respaldo en una nube. Algunos proveedores de nube con opciones gratuitas y seguras son Google Drive, Dropbox y Microsoft One Drive.

3. Establece una programación regular: Decide con qué frecuencia realizarás las copias de seguridad. Lo ideal es hacerlo de forma periódica, semanal o mensualmente, según la cantidad y la importancia de los datos.

4. Verifica la integridad de las copias de seguridad: Después de cada respaldo, verifica que los archivos estén correctamente almacenados y sean accesibles.

Píldora ¡Protege!

Jorge, jefe de despachos de la compañía de bisutería Aretes Cielo, recibe varios correos donde clientes se quejan de no haber recibido sus pedidos, y que, en los correos de confirmación enviados por el sistema, sus domicilios están errados.

Jorge no conoce los consejos de esta guía ...

1

Ingresa al módulo de despachos a revisar utilizando como contraseña 1234, que además la conocen un par de sus colaboradores.

2

Verifica que verdaderamente varias direcciones fueron modificadas.

3

Solicita le permitan la USB que utilizan para copiar archivos propios de la operación y además para copiar los archivos de la copia de seguridad.

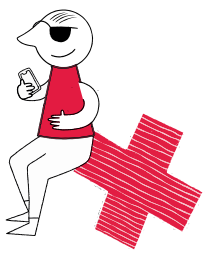
4

Al tratar de restaurar, se percata que la copia de seguridad encontrada es muy antigua, por ende, desactualizada.

5

Los pedidos fueron entregados a direcciones que desconoce; 30 pedidos distribuidos en tres direcciones de entrega.

6



Aretes Cielo fue víctima de acceso abusivo a sistema informático.

Consecuencias para Jorge

- Es responsable por la pérdida de varios pedidos por compartir información confidencial y no usar contraseñas fuertes.
- La compañía sufre de pérdida de credibilidad de sus clientes por incumplimiento en compromisos comerciales.

Píldora ¡Protege!

Jorge leyó esta guía y aplica lo aprendido ...

- Usa contraseñas fuertes y no las comparte.
- Configura el factor de autenticación de dos pasos que trae el software. El PIN de autenticación llega a su celular corporativo.
- Realiza a diario copias de seguridad en Google Drive, del módulo de despachos, incluyendo los datos de los clientes.
- Tiene el protocolo de verificar a diario con la transportadora, la recepción de los pedidos por parte de sus clientes basado en las rutas programadas.
- Cambia la clave del módulo cada tres meses.

Consecuencias para Jorge

- Evita pérdidas económicas a la compañía además de algún riesgo reputacional.
- Afina los protocolos de respaldo de información ante un factible riesgo.

Paso 4

¡Cuida!

Cuida tus redes sociales

¿Sabías que tus redes sociales empresariales están en la mira de los ciberdelincuentes?

Hoy en día, las redes sociales son una herramienta clave para las empresas, permitiéndote llegar a más clientes, darle visibilidad a productos y servicios, y construir una imagen de marca sólida. Sin embargo, este mundo virtual también presenta sus propios riesgos.

Los ciberdelincuentes han puesto sus ojos en las redes sociales de los negocios, buscando vulnerabilidades para acceder a información sensible y por supuesto, obtener réditos económicos de manera abusiva.

En este capítulo de nuestra guía, te vamos a enseñar cómo cuidar y proteger tus redes sociales de esos ataques y estafas que pueden afectar a tu negocio. Descubrirás cómo configurar de forma segura el perfil de tus redes, cómo detectar cuentas falsas y cómo establecer una buena configuración para una de las principales herramientas de las empresas hoy en día, el WhatsApp.

¡Así que prepárate para proteger tus redes sociales empresariales como un profesional y asegurar el éxito en el mundo digital!

¿Cómo configurar la privacidad nuestras redes?

Hacer del perfil de tus redes un lugar seguro es más fácil de lo que parece. Parte del desafío se encuentra en que configures de manera correcta algunos de los ajustes de privacidad de las redes sociales en las que tu negocio haga presencia. Para ello es importante que le eches un ojo a estas recomendaciones:

- **Revisa la configuración:** explora las opciones de privacidad proporcionadas por la plataforma de redes sociales que estés utilizando. Generalmente, encontrarás estas opciones en la sección de configuración o ajustes de privacidad de tu cuenta. Revisa detenidamente cada configuración y ajusta según tus necesidades.

- **Limitar la información personal visible:** Es recomendable minimizar la cantidad de información personal, como números de teléfono, direcciones de correo electrónico o datos sensibles, que esté accesible públicamente.

- **Revisar las etiquetas y menciones:** Configura las opciones para aprobar etiquetas y menciones antes de que aparezcan en el perfil de tu empresa. Esto te permitirá tener control sobre las publicaciones en las que tu empresa es etiquetada o mencionada.

- **Revisar las aplicaciones y permisos:** Elimina o revoca el acceso de las aplicaciones no utilizadas que tienen acceso a tu cuenta de redes sociales. Revisa regularmente los permisos concedidos a las aplicaciones y retira aquellos que no sean necesarios.

No olvides que muchas de las recomendaciones de seguridad del capítulo “Protege” son fundamentales en el cuidado de tus redes sociales.
Recuerda:

- Formular contraseñas fuertes de mínimo 8 caracteres, que combinen minúsculas, mayúsculas, números y caracteres especiales como #$%.
- Cambiar tus contraseñas al menos una vez cada tres meses.
- Activar la función de doble factor de verificación.

¿Cómo detectar cuentas falsas?

Las cuentas falsas en redes sociales son como impostores que quieren engañar a empresas como la tuya para estafarlas. **Los ciberdelincuentes crean perfiles falsos para hacerte creer que son personas reales o representantes de empresas legítimas.** Su objetivo es obtener información confidencial, como tus datos bancarios o contraseñas, para aprovecharse de tu negocio.

Estas cuentas falsas pueden funcionar de diferentes formas. Algunas veces se hacen pasar por empresas conocidas para ganarse tu confianza. Te pueden enviar mensajes o correos electrónicos pidiéndote información importante o haciendo ofertas que parecen tentadoras, pero en realidad son trampas. Otra

táctica es crear perfiles falsos para hacerse amigos tuyos o de tus empleados. Intentarán establecer una relación de confianza para obtener información valiosa.

Para protegerte de estas estafas, es importante estar alerta. Algunas señales de que una cuenta puede ser falsa son:

- **Si la foto de perfil de una cuenta parece ser demasiado perfecta o no tiene relación con el perfil o aparecen caricaturas, puede ser una alarma de que la cuenta es falsa.** Si desees también puedes revisar la procedencia de la imagen de la siguiente manera:

  i. Guarda la imagen en tu dispositivo.

  ii. Usa un motor de búsqueda de imágenes inversas como Google Images.

  iii. Carga la imagen en el motor de búsqueda.

  iv. Examina los resultados para ver si encuentras información sobre el origen de la imagen.

- **Si una cuenta tiene actividad sospechosa,** como publicaciones que parecen ser spam o contenido inapropiado.

- Si la información en el perfil de una cuenta es incompleta o contradictoria.

- **Si una cuenta te envía mensajes o solicitudes de amistad inesperadas,** especialmente si te pide que hagas clic en un enlace o que descargues un archivo, debes desconfiar.

- Si es una cuenta que tiene pocos y ningún posteo o publicación.

- Si no participa en ningún grupo.

- Si crees que una cuenta es falsa, puedes informarla a la plataforma de redes sociales correspondiente para sea bloqueada, previa investigación por parte de los administradores de la plataforma.

¿Cómo reducir los riesgos en WhatsApp?

En la actualidad, las pequeñas empresas han encontrado en WhatsApp una herramienta poderosa para expandir sus negocios y llegar a nuevos clientes. Estas aplicaciones de mensajería instantánea se han convertido en una plataforma de comunicación directa y efectiva para promocionar, vender y brindar servicios de manera ágil y personalizada.

WhatsApp Business, diseñada específicamente para empresas, proporciona características adicionales que facilitan la gestión de la comunicación comercial. Permite crear un perfil empresarial con información detallada, horarios de atención y enlaces a sitios web, así como automatizar respuestas a consultas frecuentes.

No obstante, al igual que con las redes sociales, **WhatsApp no se encuentra exenta de múltiples amenazas.** Algunas de las más conocidas hoy en día son el *phishing*, los virus cibernéticos, la suplantación de identidad, fugas de información e interceptaciones de mensajes.

Sigue estos consejos para configurar tu WhatsApp de manera segura y proteger tu información personal y conversaciones en la plataforma:

- **Mantén actualizada tu versión de WhatsApp** para asegurarte de tener las últimas correcciones de seguridad y mejoras.

- **Habilita el cifrado de contenido en las copias de seguridad** que realiza la plataforma en la nube.

- **Activa la verificación en dos pasos** para añadir una capa adicional de seguridad a tu cuenta.

- **Evita incluir información personal innecesaria**, como tu dirección o número de identificación en tu perfil.

- **Bloquea mensajes de números desconocidos** o no guardados en tu lista de contactos para evitar mensajes no deseados y posibles amenazas.

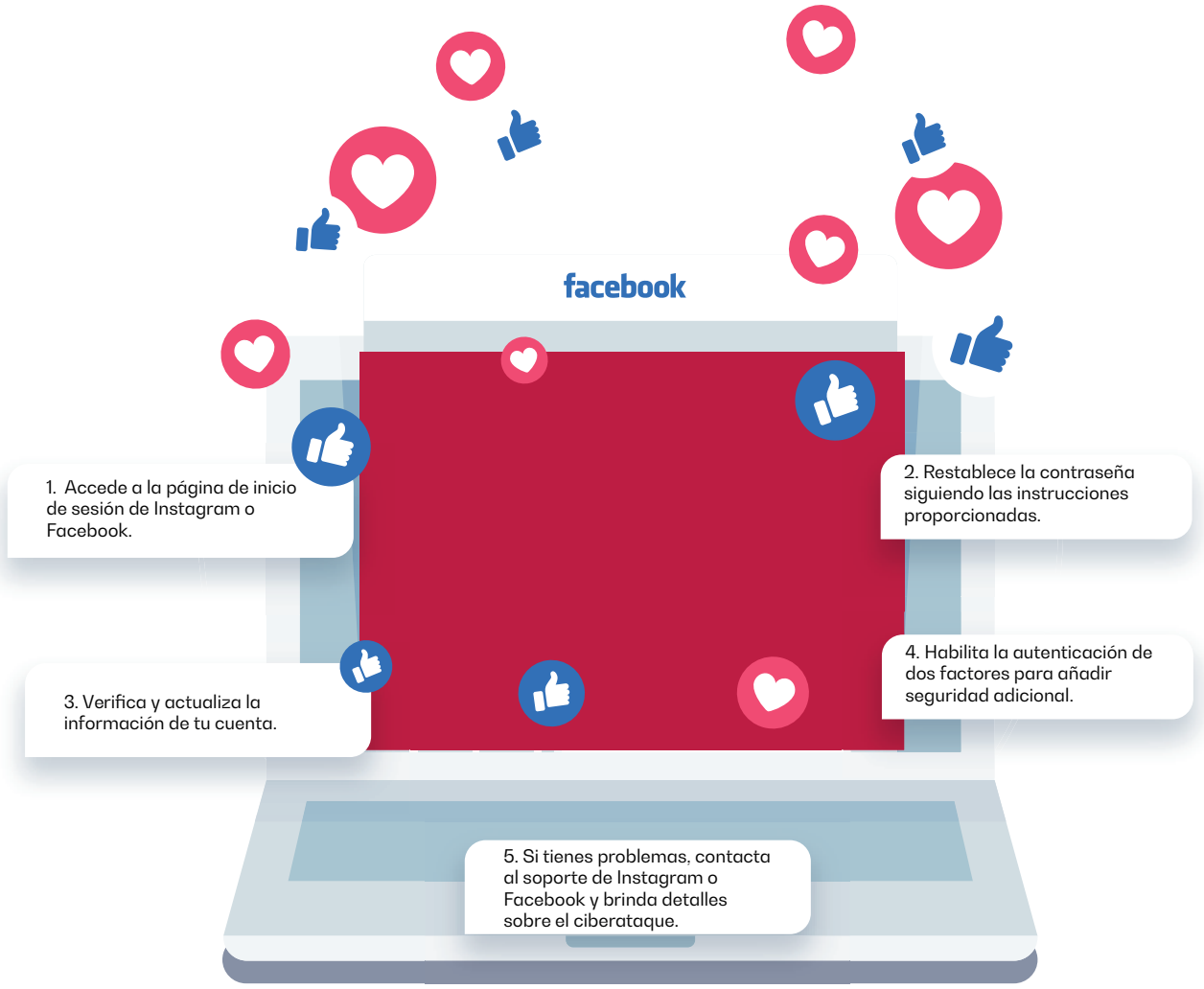
- **Configura la descarga automática de archivos multimedia** para decidir cuándo y desde dónde descargar contenido, evitando posibles virus y robo de datos.

- **Protege la privacidad de tus conversaciones** desactivando la visualización de mensajes en la pantalla de bloqueo y en las notificaciones.

- **Evita compartir información confidencial** como contraseñas o datos bancarios a través de WhatsApp.

- **Configura la privacidad de tu última conexión,** foto de perfil, estado y confirmaciones de lectura para limitar quién puede verlos.

¿Cómo recuperar la cuenta de Instagram o Facebook?

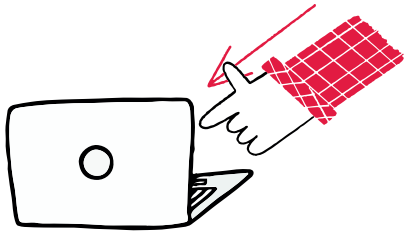


Píldora ¡Cuida!

Constanza, jefe de Marketing de la tienda de ropa "Luce Bien", acepta una solicitud de contacto en su perfil de Facebook, de "Inversiones Omega" fabricante de materias primas para el sector textil, ofreciendo unos precios demasiado bajos para el mercado. Para disfrutar de esos precios, le envían un link para diligenciar un formulario de inscripción con los datos de la empresa y de la persona de contacto.

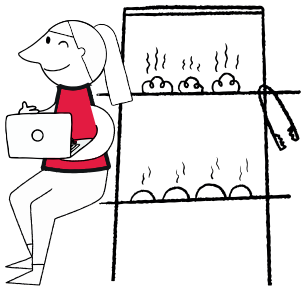
Constanza no conoce los consejos de esta guía ...

1



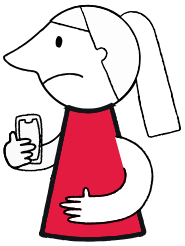
Acepta la solicitud e ingresa al link enviado, suministrando los datos solicitados.

2



Descarga la lista de productos e información de la Compañía "Inversiones Omega".

3

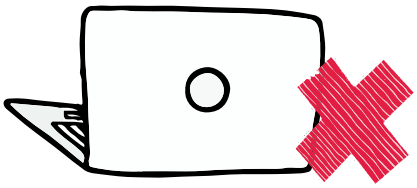


Al día siguiente al tratar de ingresar al perfil de "Luce Bien", no lo puede hacer, con la contraseña que a diario usa.

4

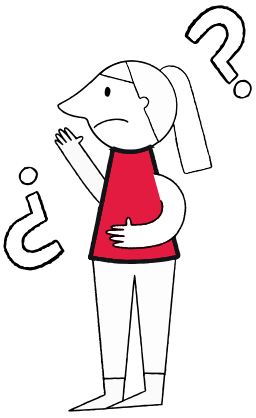
Usa la opción de "Recuperar contraseña" pero no le llega ningún correo.

5



Con la información suministrada y el archivo descargado, Constanza facilitó el robo de credenciales y su clave fue cambiada al igual que su correo de recuperación. Su perfil alterado suministrando información a sus clientes sobre una contaminación en unos lotes de su producto estrella.

6



El perfil de los ciberdelincuentes alteró la información y comete un delito por violación de datos personales.

Consecuencias para Constanza

- Facilitó una suplantación del perfil de la empresa, afectando la reputación del producto estrella de “Luce Bien”.
- Pérdidas económicas considerables, para “Luce Bien”.

Píldora ¡Cuida!

Constanza leyó esta guía y aplica lo aprendido ...

- Desconfía por los precios demasiados bajos para el mercado.
- Acepta la solicitud de contacto, pero antes de abrir el link, verifica reseñas en la web sobre esa compañía y al encontrar comentarios no apropiados, se abstiene de seguir con el proceso solicitado.
- Revisa la configuración del perfil verificando que tenga los datos básicos para ventas y verifica que se encuentre activa la verificación de dos pasos activando como segundo factor, su teléfono celular.
- Al encontrar comentarios no apropiados de este supuesto proveedor, usa la opción de reportar usuario que tiene Facebook.

Consecuencias para Constanza

- Fortalece la seguridad del perfil, aplicando consejos de esta guía.
- Evita la violación de los datos personales de su negocio.

Paso 5

¡Blinda!

Blinda tus dispositivos

¡Has llegado muy lejos! Ya estás más cerca de saber todo lo que necesitas para que tú y tu negocio reduzcan el riesgo de ser víctima de un ciberataque.

Ahora ha llegado el momento que te enteres de cómo mejorar la seguridad de tus dispositivos tanto tu computador como la de tu tablet y celular.

La importancia de blindar tus dispositivos radica en la protección de la información que contienen y el uso que en manos inescrupulosas pueda tener. Imagina que pierdes tu celular corporativo y este no cuenta con ninguna contraseña de acceso. Tus datos y los de tu negocio se encontrarán a merced de quien lo encuentre.

En esta sección de nuestra guía, aprenderás como actualizar correctamente tus dispositivos, como comprobar que están protegidos y que disponen de bloqueos de acceso. Adicionalmente, te enseñaremos como tener una gestión segura de las aplicaciones que descargas.
Es mucho más sencillo de lo que te puedas imaginar ¡Vamos por ello!

¿Cómo actualizar tus dispositivos?

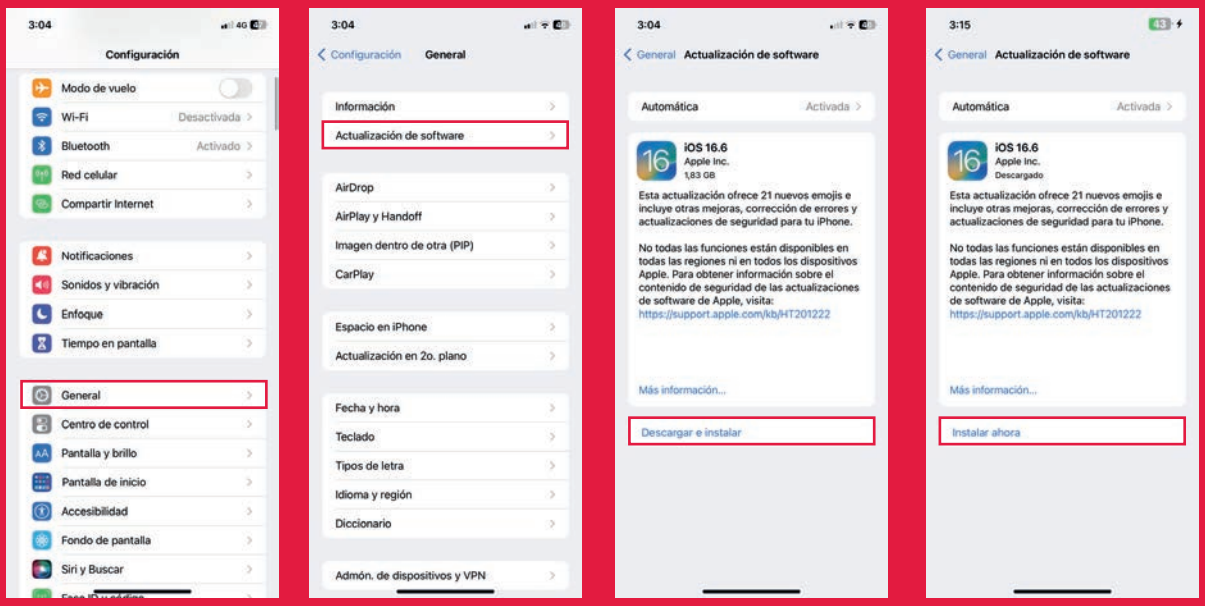
Todo software, ya sean sistemas operativos o aplicaciones deben contar con la última versión lanzada por su fabricante.

Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades, las cuales pueden ser aprovechadas por los ciberdelincuentes para acceder o comprometer el dispositivo.

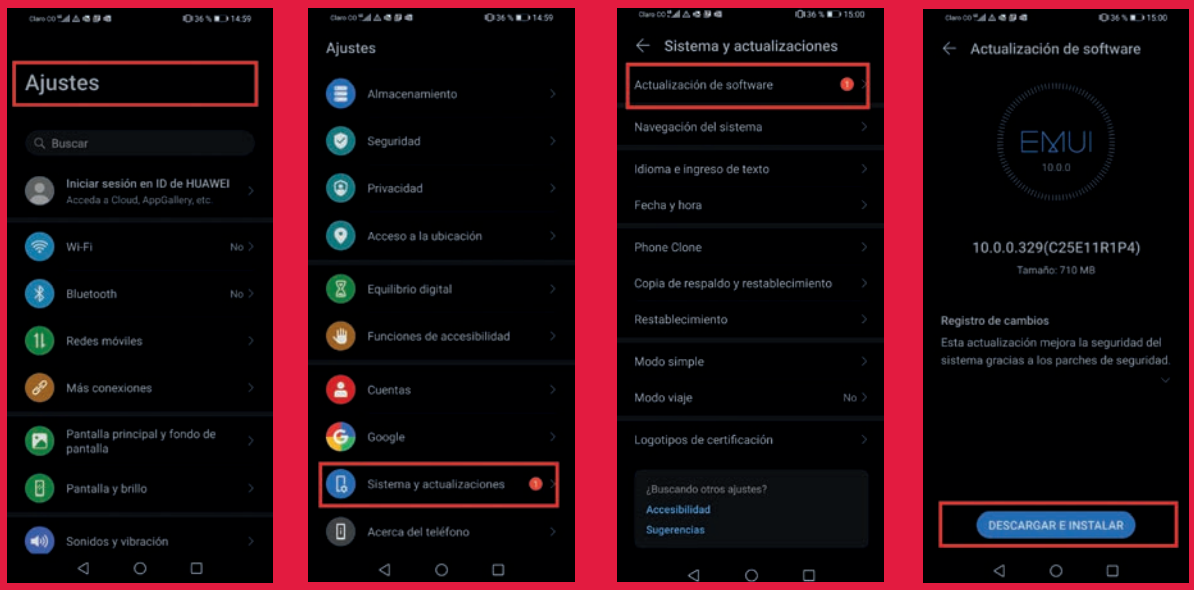
Asimismo, las actualizaciones a menudo contienen mejoras en las defensas contra programas maliciosos. Estas actualizaciones refuerzan las barreras de seguridad y ayudan a mantener los dispositivos a salvo de las últimas amenazas cibernéticas.

Computadores		Celulares y tabletas	
Windows	**Mac Os**	**IOS (iPhone y IPad)**	**Android**
1. Abre la configuración de Windows desde el menú Inicio. 2. Ve a “Actualización y seguridad”. 3. Selecciona “Windows Update”. 4. Haz clic en “Buscar actualizaciones”. 5. Si hay actualizaciones disponibles, descárgalas e instálalas. 6. Si no hay actualizaciones, tu software de Windows está actualizado.	1. Haz clic en el logotipo de Apple y selecciona “Preferencias del Sistema”. 2. Abre “Actualización de Software”. 3. Haz clic en “Actualizar ahora” si hay actualizaciones disponibles. 4. Si no hay actualizaciones, tu software macOS ya está actualizado.	1. Conecta tu dispositivo a una red Wi-Fi estable. 2. Ve a “Ajustes” > “General” > “Actualización de software”. 3. Si hay una actualización disponible, descárgala e instálala. 4. Sigue las instrucciones en pantalla. 5. Tu iPhone se reiniciará y estará actualizado. 6. Si no hay una actualización disponible, verás un mensaje que indica que tu iPhone está actualizado.	1. Abre “Ajustes” en tu dispositivo. 2. Busca “Sistema” o “Actualización de software”. 3. Toca “Buscar actualizaciones”. 4. Si hay una actualización disponible, descárgala e instálala. 5. Sigue las instrucciones en pantalla. 6. Si no hay actualizaciones disponibles, tu celular Android está actualizado.

Iphone



Android



¿Cómo comprobar la protección de tus dispositivos?

Asegurarte de contar con la última versión actualizada disponible es muy importante, pero revisar las condiciones de protección y seguridad de tus dispositivos también es fundamental.

La importancia de verificar que nuestros dispositivos estén protegidos radica en que no tengamos aplicaciones instaladas sin nuestro consentimiento, que puedan tener comportamientos maliciosos y que incluso puedan infectar otros dispositivos.

Si bien, la principal barrera de protección de nuestros equipos son sus actualizaciones y el correcto funcionamiento de un antivirus, existen algunos elementos adicionales a los que debes prestar atención.

Para este caso en particular, no existe una ruta general para sistemas operativos y dispositivos, ya que cada fabricante ofrece diferentes opciones de verificación de la protección.

Chequea periódicamente las siguientes opciones dependiendo el sistema operativo de tu dispositivo:

1. En Windows:

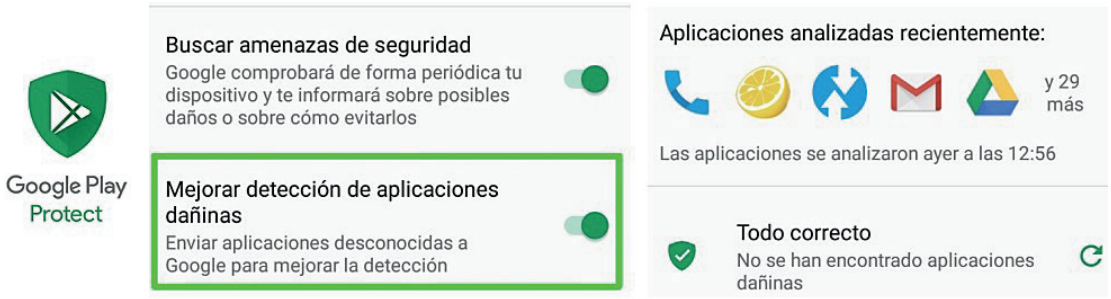
Debes ingresar a configuración haciendo clic en el botón "Windows" en la parte inferior izquierda y selecciona la opción de "Actualización y seguridad". Verifica que la lista de chequeo que se despliega contiene chulitos verdes. De lo contrario, presiona la categoría y sigue las acciones recomendadas.

2. En Mac OS:

Haz clic en el logotipo de Apple y selecciona "Preferencias del Sistema" y luego el icono que dice "Seguridad y privacidad". Debes verificar que la opción Firewall se encuentre activada.

3. En Android:

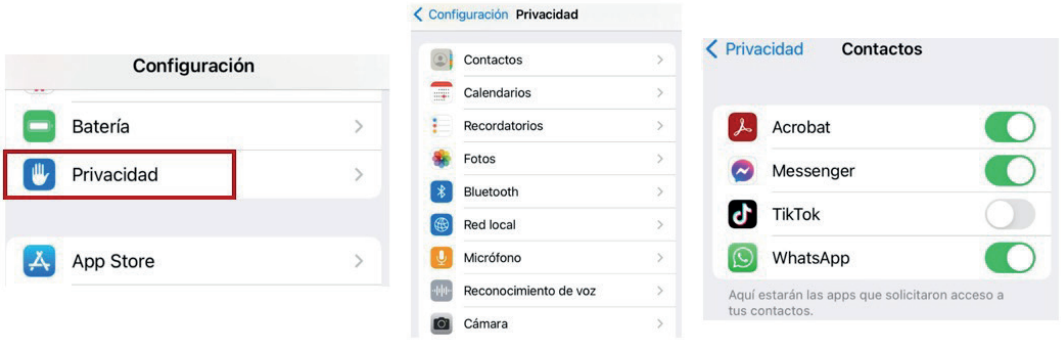
Por defecto trae una herramienta llamada Google Play Protect y debemos verificar que esté instalada y actualizada dentro del sitio oficial llamado Play Store del que normalmente descargas aplicaciones.



4. En IOS:

La principal protección en este sistema operativo es el filtro que nos brindan las aplicaciones contenidas en App Store, no obstante, es importante que verifiques los permisos de acceso que tienen las aplicaciones instaladas en tu dispositivo.

Debemos ingresar a "Configuración General" y luego presionar "Privacidad". Podrás observar todas tus aplicaciones y los permisos que tienen de acceder a tu lista de contactos, ubicación, cámara, álbum de fotos, etc. Verifica que cada aplicación acceda únicamente a lo que es estrictamente necesario con su funcionalidad. ¿Para qué debería acceder una aplicación que edita fotos a tu lista de contactos?



¿Cómo configurar bloqueos de acceso?

El bloqueo de acceso es una configuración de seguridad, que como su nombre indica, impide el acceso no autorizado a un dispositivo, bien sea computador, tableta o celular.

En otras palabras, u**n bloqueo de acceso en un computador o celular es como tener una cerradura en la puerta de tu casa.** Utilizas una contraseña, un patrón de desbloqueo o tu huella digital para asegurarte de que solo tú puedas acceder al dispositivo.

Esto ayuda a mantener tus datos y la información personal que tienes en el dispositivo seguros y privados, evitando que otras personas puedan ver o usar tus cosas sin tu permiso.

Es fundamental que todos tus dispositivos cuenten como mínimo con un bloqueo de acceso en forma de contraseña o verificación facial o de huella. Igualmente es importante que automatices el bloqueo automático de la pantalla en máximo 1 minuto. Esto garantiza que tu dispositivo siempre se encuentre bloqueado cuando no lo estás usando.

Dependiendo el tipo de dispositivo puedes revisar y configurar el tipo de bloqueo de acceso que más te convenga y el tiempo de bloqueo automático de la siguiente manera:

Computadores		Celulares y tabletas	
Windows	**Mac Os**	**IOS (iPhone y IPad)**	**Android**
1. Haz clic en el botón de “Inicio” y selecciona “Configuración”. 2. Ve a “Cuentas” y luego a “Opciones de inicio de sesión”. 3. Elige una opción de bloqueo de acceso, como contraseña, PIN o reconocimiento facial. 4. Configura la opción seleccionada siguiendo las instrucciones en pantalla. 5. Vuelve a la “Configuración”. 6. Ve a “Sistema” y luego a “Energía y suspensión”. 7. Establece el tiempo deseado en “Apagar la pantalla después de” para que se bloquee automáticamente.	1. Haz clic en el menú de Apple y selecciona “Preferencias del Sistema”. 2. Ve a “Seguridad y privacidad”. 3. Desbloquea la configuración haciendo clic en el candado. 4. Elige una opción de bloqueo de acceso, como contraseña, Apple Watch o Touch ID. 5. Configura la opción seleccionada siguiendo las instrucciones en pantalla. 6. En esta misma opción elige el tiempo de inactividad deseado para que la pantalla se bloquee de manera automática.	1. Abre la aplicación “Configuración” en tu dispositivo iOS. 2. Ve a “Face ID y código” o “Touch ID y código”. 3. Establece un código de acceso de al menos seis dígitos. 4. Configura el desbloqueo biométrico (Face ID o Touch ID) si está disponible. 5. Activa la opción “Requerir código” para mayor seguridad. 6. Abre nuevamente “configuración” y ve a “Pantalla y Brillo”. 7. Selecciona “Bloqueo automático” y elige el tiempo de inactividad deseado antes de que la pantalla se bloquee automáticamente.	1. Abre la aplicación “Configuración” en tu dispositivo Android. 2. Ve a “Seguridad” o “Bloqueo de pantalla”. 3. Elige una opción de bloqueo de acceso, como “Patrón”, “PIN”, “Contraseña” o “Huella digital”. 4. Sigue las instrucciones en pantalla para configurar el bloqueo de acceso seleccionado. 5. Activa la opción “Bloqueo automático” y elige el tiempo de inactividad antes de que se bloquee la pantalla.

¿Cómo descargar aplicaciones y programas sin riesgo?

¿Podemos estar en peligro cuando descargamos aplicaciones y/o programas en nuestros dispositivos? La respuesta es: por supuesto que sí.

Las aplicaciones maliciosas son una de las tantas formas que usan los ciberdelincuentes para poder infectar tu dispositivo y tomar control de tu información con fines perversos. Es por esto por lo que cada vez que vayas a descargar un programa en tu computador, o una aplicación en tu dispositivo móvil, ten en cuenta las siguientes recomendaciones:

1. Utiliza fuentes confiables: Descarga programas y aplicaciones solo desde fuentes oficiales, como las tiendas de aplicaciones oficiales (como App Store para iOS y Google Play Store para Android) o los sitios web oficiales de los desarrolladores.

2. Verifica las reseñas y calificaciones: Esto te ayudará a tener una idea de la calidad y seguridad de la aplicación.

3. Ten cuidado con los permisos: Si una aplicación solicita más permisos de los necesarios para su funcionalidad, es posible que debas reconsiderar su instalación.

4. Evita descargar desde enlaces sospechosos: No descargues programas o aplicaciones de enlaces que recibas a través de mensajes de correo electrónico no solicitados o sitios web desconocidos. Estos enlaces pueden ser potencialmente peligrosos y contener programas maliciosos.

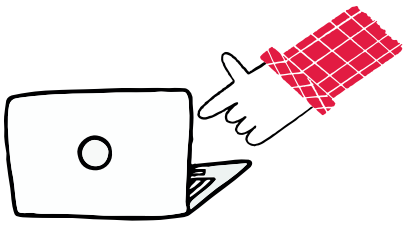
5. Lee los términos y condiciones: Antes de instalar una aplicación, lee los términos y condiciones, así como la política de privacidad. Asegúrate de comprender cómo se utilizarán tus datos personales y qué permisos estás otorgando.

Píldora ¡Blinda!

Carlos, diseñador gráfico de empresa de domicilios “Pronta Entrega”, necesita descargar un software de imágenes que no tenga costo. Busca por Google dicho software encontrando múltiples direcciones. Selecciona un link que lo lleva a una página de descargas libres. En el proceso de instalación recibe un mensaje que le informa que se instalará un software adicional que le ayudará en inversiones en la bolsa de valores.

Carlos no conoce los consejos de esta guía ...

1



En el proceso de instalación hace clic en OK a todos los mensajes que aparecen en el proceso.

2

El software de imágenes y el software adicional se instalan en las carpetas respectivas.

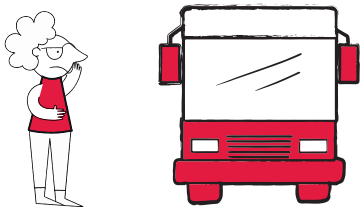
3

El software adicional, instala un programa espía dentro del equipo y toma control de los contactos de WhatsApp.

4

Días después les llegan a sus contactos mensajes, solicitando sumas de dinero no mayores a $ 200.000 para salir de un impase y prometiendo devolverlos al día siguiente. En el mensaje se incluye un numero de una app de pagos en link para realizar la transferencia.

5



Carlos y Pronta Entrega son víctimas del delito de Interceptación de datos informáticos.

Consecuencias para Carlos

- El software que se instaló con su consentimiento, instalo un virus que espiaba toda la información contenida en el equipo.
- Algunos de sus contactos perdieron pequeñas sumas, pero queda el sin sabor de haber sido robados después de que se enteran de lo que realmente sucedió.

Píldora ¡Blinda!

Carlos leyó esta guía y aplica lo apren-

- Analiza el mensaje y se da cuenta que el dominio de la URL no coincide con el dominio del fabricante.
- Verifica que el navegador que usa esté actualizado.
- Analiza los resultados que trae la búsqueda y selecciona el que coincide con el dominio del fabricante del software.

- Verifica antes de la descarga, que el antivirus esté activo y actualizado.
- Ingresa a la página web del fabricante, verifica seguridad en la URL y selecciona el archivo para descargar e instalar el software.
- Instala exclusivamente el software de imágenes.

Consecuencias para Carlos

- Le recuerda que antes de realizar descargas de software, debe hacer verificaciones, como que el antivirus esté activo y que los dominios coincidan con el dominio del fabricante.

Paso 6

¡Denuncia!

Denuncia si eres víctima de un ciberdelito

¡Lo lograste! Ya has aprendido las medidas preventivas en ciberseguridad más importantes. Ahora, es fundamental que compartas con tus colaboradores e incluso tu familia todos estos tips y recomendaciones para que el riesgo de sufrir un ciberataque se reduzca sustancialmente.

No te vayas, nos falta una última tarea, que más que preventiva corresponde a un valor civil y que será un insumo fundamental para que las autoridades del gobierno puedan hacer política pública para combatir a los ciberdelincuentes. Este trabajo final es denunciar cualquier tipo de ciberdelito del que tú y tus negocios sean víctima.

Por una parte, **al denunciar un ciberdelito, estás protegiendo tus propios derechos e intereses.** Si has sido víctima de un delito en línea, como el robo de identidad, el fraude en la web o el acoso cibernético, al informar a las autoridades, puedes obtener apoyo para resolver el problema y salvaguardar tu seguridad personal.

Asimismo, las autoridades competentes en Colombia cuentan con unidades especializadas en delitos informáticos que tienen la experiencia y los recursos necesarios para investigar los ciberdelitos. Al presentar una denuncia, estás contribuyendo a la investigación y proporcionando información clave que puede ayudar a identificar a los delincuentes y llevarlos ante la justicia.

Por otra parte, **cuando denuncias ayudas a prevenir que otros sean víctimas de la misma actividad delictiva.** Tu denuncia puede proporcionar pruebas valiosas para identificar y detener a los delincuentes, así como para desmantelar redes criminales más grandes.

Las denuncias de ciberdelitos permiten recopilar datos y estadísticas sobre las tendencias delictivas en línea. **Estos datos son fundamentales para comprender la magnitud del problema, desarrollar estrategias de prevención más efectivas y asignar recursos adecuados para combatir los ciberdelitos en el futuro.**

En esta última sección, te contamos los sencillos pasos que debes seguir para interponer una denuncia cuando hayas sido víctima de un delito cibernético, así como los mecanismos para hacer seguimiento de esta.

¿Cómo denunciar un delito cibernético?

Interponer una denuncia de un ciberdelito es mucho más sencillo de lo que puedas imaginar. Desde 2016, Colombia cuenta con un aplicativo de denuncia virtual llamado a **ADenunciar.** Esta robusta plataforma tiene una sección para denunciar delitos cibernéticos. Incluso cuando el ciudadano no tiene claridad de que tipo de delito fue víctima, el aplicativo formula una serie de preguntas sencillas que van dando una guía

Entonces, si consideras que fuiste víctima de alguno de los diferentes ataques que hablamos a lo largo de esta guía, sigue este paso a paso:

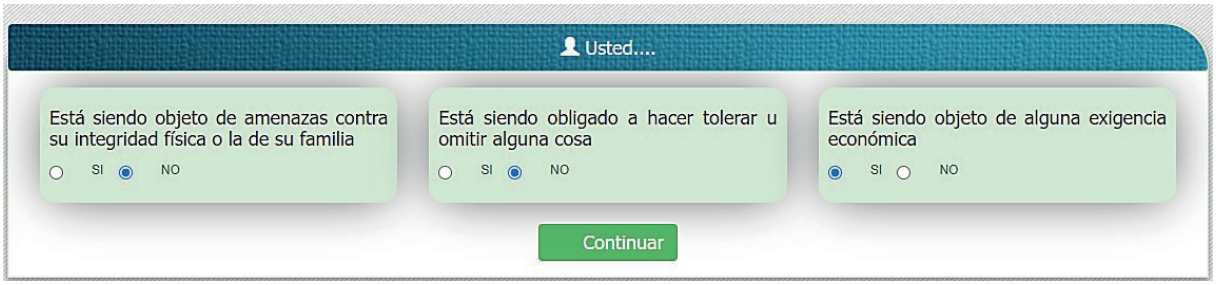
1. Ingresa a la plataforma ADenunciar aquí o a través del siguiente código QR:

2. Selecciona la opción “Denuncia virtual”.

3. Aparecerá una ventana donde se señalan los “Términos y Condiciones” sobre el manejo de la plataforma en datos personales. Haz clic en “Aceptar” y continua.

4. **Selecciona la opción “Delitos Cibernéticos”.** Se desplegará una nueva ventana informativa que explica brevemente que son estos delitos. Haz clic en “Continuar”.

5. El sistema señala tres preguntas de Sí o No que deben ser respondidas con el fin de establecer si efectivamente has sido víctima de un ciberdelito. Responde estas preguntas y haz clic en “Continuar”:



6. **Al responder Sí, en al menos de una de las tres preguntas, será por que efectivamente pudiste ser víctima de un ataque cibernético** por lo que el sistema arrojará una ventana informativa en el que se señalan los derechos y deberes que tienes una vez se interponga la denuncia. Haz clic en “OK”.

7. Responde Sí o No a la pregunta “¿Sabe si estos hechos han sido puestos en conocimiento de una autoridad?”. Selecciona el botón “Continuar”.

8. Completa tus datos personales y selecciona” Continuar”.

Si respondes No a las tres preguntas, el sistema arrojará un mensaje señalando que no has sufrido un delito cibernético. En este caso es posible que estes siendo víctima de otra clase delito como una extorsión, una estafa o un hurto común. Es por ello por lo que es importante que te asesores para saber que delito denunciar a través de la línea de la Policía Nacional 018000-910112.

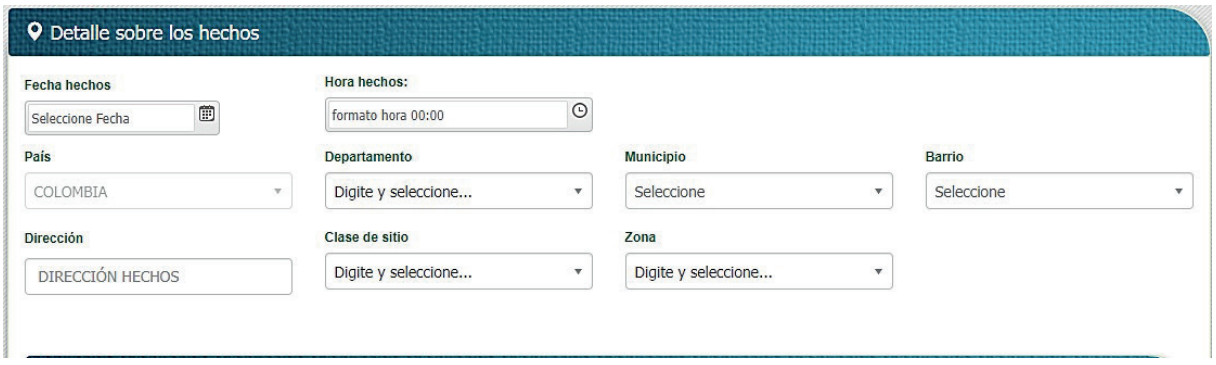
9. Completa tus datos generales y haz clic en “Continuar”.

10. Completa tus datos de contacto y presiona el icono “Siguiente”.

11. Contesta seis preguntas de Sí o No que indican:

- ¿Fuiste tú la víctima?
- ¿Hay víctimas adicionales?
- ¿Tienes información de la persona que cometió el delito?
- ¿Eres testigo?
- ¿Existen testigos adicionales de los hechos?

12. Señala el detalle sobre los hechos. Esto significa mencionar fecha, lugar y hora donde ocurrieron.



13. Indica el relato de los hechos sin obviar ningún detalle. Haz clic en “Continuar”.

Relato de los hechos

CON EL FIN DE COMPLEMENTAR DE MANERA DETALLADA Y PRECISA LA DESCRIPCIÓN DE LOS HECHOS QUE ACABA DE RELATAR, POR FAVOR RESPONDA LAS SIGUIENTES PREGUNTAS:

Realice una descripción detallada de los hechos que va a denunciar.

RECUERDE QUE ESTE CAMPO ES OBLIGATORIO Y TIENE UN MAXIMO DE 3800 CARACTERES

1. ¿Cuándo y cómo se enteró de que había sido víctima de este delito informático?

2. ¿Sabe o sospecha de alguien?

3. ¿Sabe dónde se puede ubicar a esta persona? (ejemplo: ID, nombre de usuario o URL de redes sociales; correo electrónico, páginas de internet, celular, etc.)

4. ¿Alguna tarjeta de crédito o débito, cuenta de ahorro o corriente, o producto financiero, estuvo comprometido en el hecho?

SI NO

5. Si ha abierto correos sospechosos, indique el correo remitente y describa su contenido

6. Si ha ingresado a alguna página de internet sospechosa, indique la dirección (URL) y/o nombre de la página.

7. Si ha descargado programas gratuitos, indique el nombre y dirección de la página de internet de la que realizó la descarga.

8. Si ha recibido algún tipo llamada telefónica sospechosa, indique el número, fecha, nombre de la persona o empresa, y tipo de datos solicitados

9. Indique si hubo pérdidas económicas y de qué valor..

10. Indique si tuvo otra afectación diferente o adicional a la pérdida económica

11. ¿Ha reportado a la entidad financiera lo sucedido?

12. ¿Qué respuesta obtuvo por parte de la entidad financiera?

13. ¿La entidad financiera ha iniciado alguna investigación interna sobre los hechos?

14. Señala el tipo de conducta del que consideras que fuiste víctima entre:

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Si no tienes claridad sobre ello, puedes seleccionar la opción “No Aplica”

15. Selecciona el sector al que perteneces e indica alguna otra observación que quieras hacer. Haz clic en “Continuar”.

16. Adjunta archivos de imagen, video o audio que consideras importantes para validar el delito. Haz clic en “Enviar”.

17. Finaliza haciendo clic en el botón “Continuar” sobre la ventana informativa que se despliega.

¿Cómo hacer seguimiento a una denuncia?

Al finalizar el proceso de denuncia el sistema te indicará un número incidente como este: DI-25-322-2023-12756. Es fundamental que lo anotes y lo tengas contigo.

En las 24 horas próximas al registro se te informará a tu correo electrónico el resultado de la verificación realizada. Si los hechos relatados en este incidente corresponden a un delito, se creará la denuncia y la Fiscalía General de la Nación será la entidad encargada de continuar con el trámite correspondiente.

Si requieres información sobre una denuncia, comunícate con la Fiscalía General de la Nación a la línea nacional gratuita 018000919748, Bogotá 6015702000 opción 7 y celular gratuito 122.

Píldora ¡Denuncia!

Paula es la jefe de Compras de la comercializadora de alimentos "El Amanecer". Como una de sus tareas revisa y contesta las propuestas económicas de posibles proveedores. Uno de los correos revisados traía un link el cual activó, entregó datos sensibles y fue víctima de *Phishing*. Varios computadores fueron infectados por el virus instalado que se propagó por la red.

Paula no conoce los consejos de esta guía ...

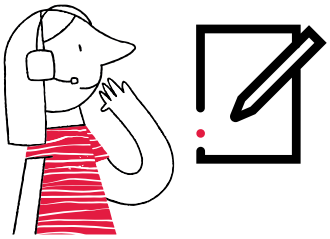
1

Se limitó a informar al área de Sistemas sobre un bloqueo en su cuenta de correo. También sobre clientes que están recibiendo correos del dominio @elamanecer.com, que han sido detectados y bloqueados por sus antivirus por considerarlos como correos maliciosos.

2

Una vez le informan de Sistemas que fue víctima de *Phishing*, se limita solicitar solucionen el problema, pero nunca denuncia ante las autoridades.

3



La opción de autocompletado también estaba activa.

4

No es consciente de la sensibilidad de la información que está almacenando en su portátil.

Consecuencias para Paula

- Alto riesgo reputacional por exposición de información privada de sus clientes.
- Aplicación de la ley de protección de datos y factibilidad de multas y suspensión de licencia de funcionamiento de su negocio.

Píldora ¡Denuncia!

Paula leyó esta guía y aplica lo aprendido ...

- Pide ayuda al área de Sistemas para saber exactamente qué está pasando con los correos.
- Al ser informada sobre la modalidad de ataque de la cual fue víctima, pide información técnica al área de IT para poder formular la denuncia en la plataforma virtual ADenunciar.
- En 15 minutos siguió el paso a paso del aplicativo de denuncia virtual. Relató con detalle los hechos y adjuntó pruebas como imágenes del correo electrónico que recibió y las alertas de virus de varios computadores.

Consecuencias para Paula

- Colabora con las autoridades para que las investigaciones hagan posible la captura y amplíen el conocimiento sobre nuevas modalidades de ataque usados por estas organizaciones de cibercrimen.

Lista de chequeo final

¿Qué tan ciberseguro eres hoy?

¡Responde este breve cuestionario!

¡Mide tu nivel de riesgo!

¡Toma acciones correctivas!

Sección Guía	Pregunta		Respuesta	
			SI	NO
Paso 1: ¡Conoce!	1	¿Verificas en los correos electrónicos recibidos que el dominio coincida con el remitente?		
	2	¿Desconfías de los correos que contienen archivos adjuntos con extensiones desconocidas?		
	3	¿Verificas los enlaces que vienen en lo mensajes de texto recibidos en tu celular antes de abrirlos?		
	4	¿Verificas la composición de las URL en las páginas donde navegas? (https://)		
	5	¿Verificas la reputación del comprador en reseñas y comentarios realizados por otros vendedores?		
	6	¿Digitas manualmente las direcciones Web a donde quieres ingresar?		
Paso 2: ¡Navega!	7	¿Evitas conectarte a Wifi gratuitas disponibles en sitios públicos?		
	8	¿Cambias periódicamente la clave de tu router?		
	9	¿Usas el modo incognito cuando navegas por internet?		
	10	¿Verificas las actualizaciones de tus navegadores de Internet?		
Paso 3: ¡Protege!	11	¿Usas contraseñas fuertes en tus accesos y cuentas personales?		
	12	¿Configuras tus cuentas con autenticación de dos pasos?		
	13	¿Realizas copias de seguridad periódicamente de tu información relevante?		
Paso 4: ¡Cuida!	14	¿Verificas los permisos de privacidad con los que cuentas los perfiles de tus redes sociales?		
	15	¿Verificas en tus dispositivos que la versión de WhatsApp sea la última disponible?		
Paso 5: ¡Blinda!	16	¿Revisas que los sistemas operativos de tus dispositivos tengan instaladas las últimas versiones?		
	17	¿Disponen tus dispositivos de bloques de acceso ya sean contraseñas, Face Id, huellas?		
	18	¿Descargas aplicaciones de sitios pertenecientes a los fabricantes del software que requieres?		
Paso 6: ¡Denuncia!	19	¿Denuncias ante las autoridades cuando se materializa un evento de seguridad en tu empresa?		
	20	¿Haces el debido seguimiento que nos facilita la plataforma de la autoridad competente?		
		TOTAL		

Ten en cuenta que dependiendo del número de NO que respondas, tu nivel de riesgo en ciberseguridad pueda variar de la siguiente manera:

- Riesgo Alto: Respondiste 13 o más veces No.
- Riesgo Medio: Respondiste entre 6 y 12 veces No.
- Riesgo Bajo: Respondiste menos de 6 veces No.

En cualquiera de estos casos, corrige estas costumbres. Vuelve a la sección de la guía de la pregunta que respondiste de manera negativa y toma las recomendaciones y tips que allí se encuentran.

Anexos

ANEXO 1

Modelo de formato de protección de datos personales

[Nombre de la empresa o entidad]
[NIT de la empresa]
[Dirección de la empresa]
[Ciudad, Código Postal]
[Teléfono de contacto]
[Correo electrónico de contacto]
[Página web]

Yo, [Nombre completo del titular de los datos], identificado(a) con [Tipo y número de documento de identificación], en calidad de titular de los datos personales, autorizo a [Nombre de la empresa] para el manejo y tratamiento de mis datos personales, de acuerdo con lo establecido en la Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios.

1. FINALIDAD DEL TRATAMIENTO

Autorizo a [Nombre de la empresa] para tratar mis datos personales con la siguiente finalidad: [Describir detalladamente la finalidad del tratamiento, por ejemplo: gestión de clientes, proveedores, envío de información comercial, análisis estadístico, entre otros.]

2. DATOS PERSONALES OBJETO DE TRATAMIENTO

Autorizo el tratamiento de los siguientes datos personales:

- Nombre completo:
- Documento de identificación:
- Fecha de nacimiento:
- Dirección:
- Teléfono:
- Correo electrónico:

3. DERECHOS DEL TITULAR DE LOS DATOS

Reconozco que como titular de los datos personales tengo los siguientes derechos:
- Derecho de acceso: Acceder a mis datos personales y conocer la información relacionada con su tratamiento.
- Derecho de rectificación: Solicitar la actualización o corrección de mis datos personales en caso de ser inexactos o incompletos.
- Derecho de cancelación: Solicitar la eliminación de mis datos personales cuando considere que no se requieren para los fines establecidos o que su tratamiento no cumple con las disposiciones legales y reglamentarias.
- Derecho de oposición: Oponerme al tratamiento de mis datos personales por motivos particulares.
- Derecho de limitación del tratamiento: Solicitar la limitación del tratamiento de mis datos personales en ciertas circunstancias.
- Derecho de portabilidad: Solicitar la entrega de mis datos personales en un formato estructurado, de uso común y lectura mecánica, o su transferencia a otra entidad.

4. SEGURIDAD DE LOS DATOS PERSONALES

Reconozco que [Nombre de la empresa] ha adoptado las medidas técnicas, administrativas y organizativas necesarias para garantizar la seguridad y confidencialidad de mis datos personales, con el fin de evitar su pérdida, uso indebido, acceso no autorizado o alteración.

5. TRANSFERENCIA DE DATOS PERSONALES

Autorizo a [Nombre de la empresa] para transferir mis datos personales a terceros, dentro o fuera del territorio colombiano, en cumplimiento de la finalidad establecida en este formato.

6. PLAZO DE CONSERVACIÓN

Mis datos personales serán conservados por [Nombre de la empresa] durante el tiempo necesario para cumplir con la finalidad establecida en este formato y conforme a las disposiciones legales y reglamentarias aplicables.

7. REVOCACIÓN DE LA AUTORIZACIÓN

Tengo el derecho de revocar en cualquier momento la autorización otorgada para el tratamiento

Se firma en la ciudad de _____, a los ___ días del mes de _____ del año____.

Firma: _____

Nombre: _____

Identificación: _____

Cámara de Comercio de Bogotá

CCB.ORG.CO

camaracomerbog