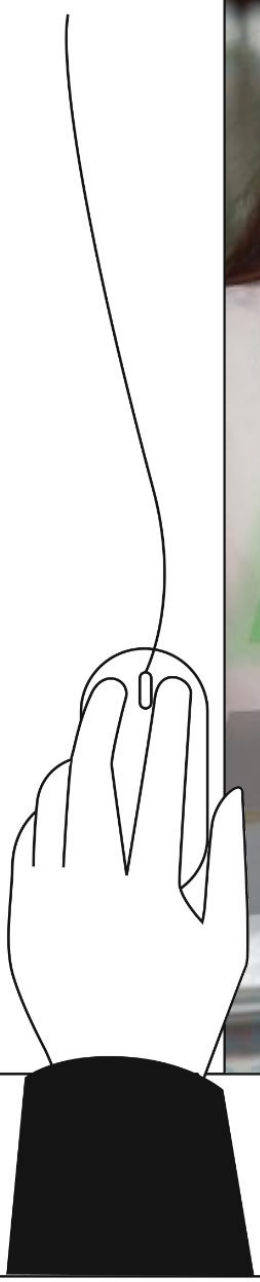
vuela

CIBERSEGURIDAD

¡Navega hacia una Internet Segura!



Junta de Andalucía

Agencia Digital de Andalucía

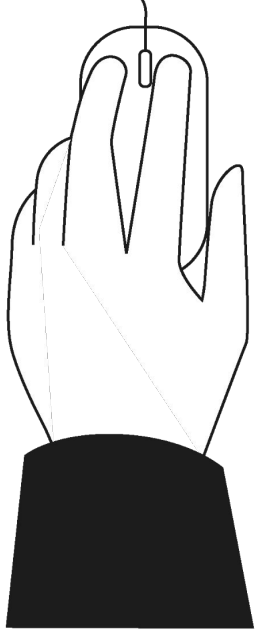
1

Identifica las amenazas..... 4

2

Protégete ante los riesgos..... 62

info



3

Aumenta tu seguridad con las herramientas adecuadas..... 109

4

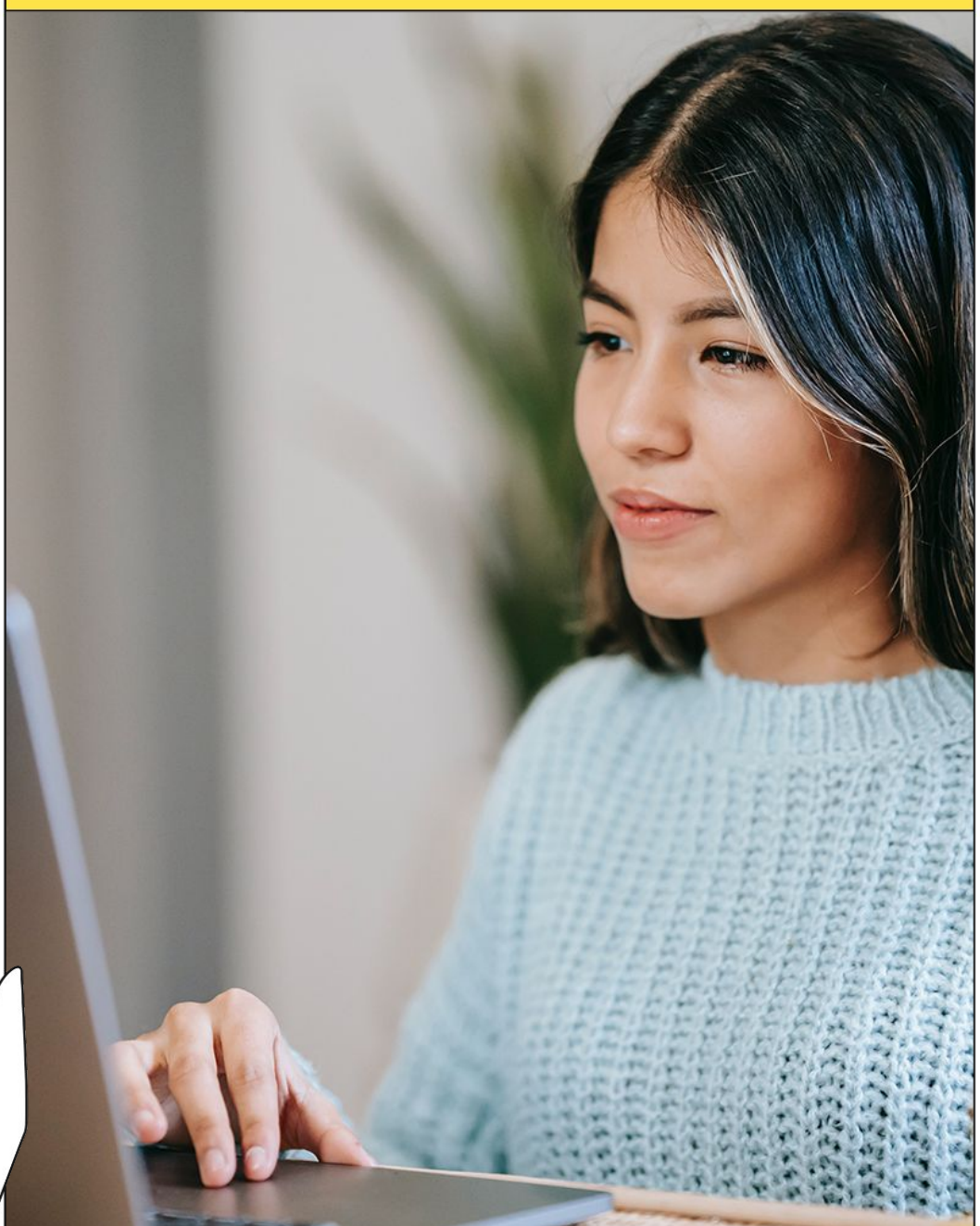
Resuelve tus problemas más frecuentes.....160

vuela

Identifica las amenazas

Aprende a identificar las amenazas más comunes en Internet. En este primer apartado te mostramos cómo conociendo los riesgos y evitando algunos comportamientos puedes mejorar fácilmente tu seguridad informática.

1



Junta de Andalucía

Agencia Digital de Andalucía

vuela

1.1

Datos personales: cómo evitar dar información personal en la red

Junta de Andalucía

Agencia Digital de Andalucía

¿Sabes qué datos personales tuyos circulan por la red?

Internet el mayor banco de información jamás creado. Esto brinda muchas oportunidades para el aprendizaje y el entretenimiento, pero también nos invita a navegar con responsabilidad y a tomar algunas precauciones para que nuestros datos personales o información sensible no acaben formando parte de ese banco de información universal que es la red.

Por esta razón, es importante que conozcas tanto qué información personal ya se encuentra en la red como la forma de evitar la publicación no deseada de datos privados. En esta guía descubrirás cómo detectar la información relacionada contigo que existe en Internet, los riesgos que conlleva y las medidas para evitar estas filtraciones. De esta forma, navegarás con mayor seguridad y control sobre tus datos en el futuro.

¿Qué información tuya existe en Internet?

En un primer momento, parece que la **privacidad en Internet** está garantizada. Al fin y al cabo, pasar desapercibido en el anonimato es más sencillo. Sin embargo, **cada persona que usa Internet deja una huella digital (un rastro de información con todo lo que hacemos en la red) al utilizar este servicio**, ya sea consciente o no de ello. De hecho, puedes comprobarlo con solo poner tu nombre en un buscador.

Esto no debe asustarte, ya que **es posible que aparezcas por un perfil en alguna red social**. Por otro lado, si te matriculaste en una facultad o curso, quizás se muestren las listas en la web de la organización. Sin embargo, las modificaciones en la Ley de Protección de Datos tienden a restringir la aparición de esta información en la red, junto a tu propio DNI.

Tampoco te costará encontrar dónde estudiaste o tu localización. **Estos datos suelen mostrarse en las propias redes sociales;** es decir, son datos que facilitamos activamente a la red. Las fotografías son otra forma de mostrar información personal. Por tanto, puedes disponer de una buena cantidad de información propia en la red casi sin darte cuenta.

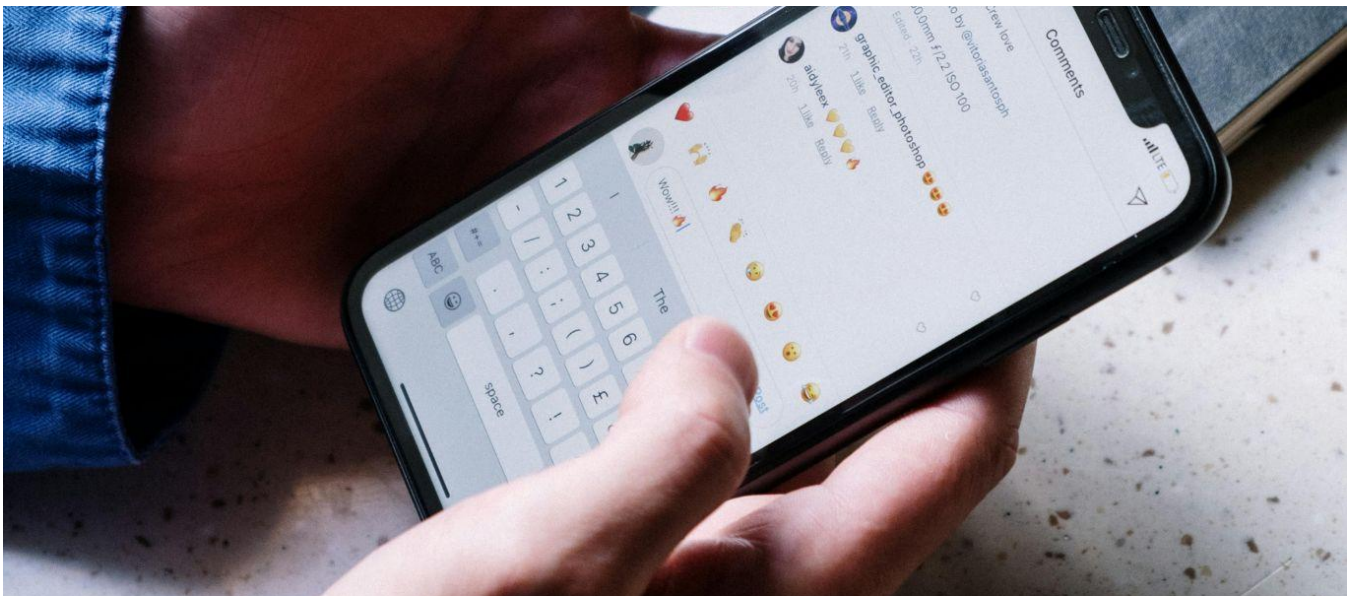
El riesgo de publicar información sin cautela

Como has visto, publicar información personal en Internet es relativamente simple, aunque los avances legislativos mejoran la privacidad. **Un primer riesgo es que tus datos llegarán a otras personas desconocidas**. Aunque esto no tiene que implicar necesariamente ser víctima de ningún tipo de ataque informático, siempre es mejor tomar medidas preventivas, ya sea para evitar a los y las ciberdelincuentes o para cuidar nuestra reputación *online*.

Otro riesgo importante de la publicación descuidada de información personal es que **simplificas la posibilidad de que te rastreen**. Esto no solo permite a ciberdelincuentes encontrar más información tuya, sino que la pueden emplear ladrones convencionales. Por ejemplo, si publicas tus fotos de las vacaciones en tu red social en abierto, estás informando de que no estás en casa. También podrías mostrar tu dirección sin querer.

A su vez, podrías sufrir ciberacoso. Al ofrecer datos como tu nombre y apellidos, **una persona con la suficiente habilidad puede llegar a encontrar formas de contactarte**. Como en el caso anterior, es muy probable que esto no ocurra nunca, pero este tipo de acoso tiene el potencial de ser grave. Podrías recibir burlas en tus perfiles, mensajes a horas incómodas o la difusión de rumores negativos sobre ti.

Por descontado, **te expones a que suplanten tu identidad o a que te roben tus perfiles en las redes sociales u otras plataformas**. Al rastrear tu información, una actividad que puede desarrollarse durante meses, las personas que tengan interés pueden acabar por localizarte en diferentes espacios de la red.

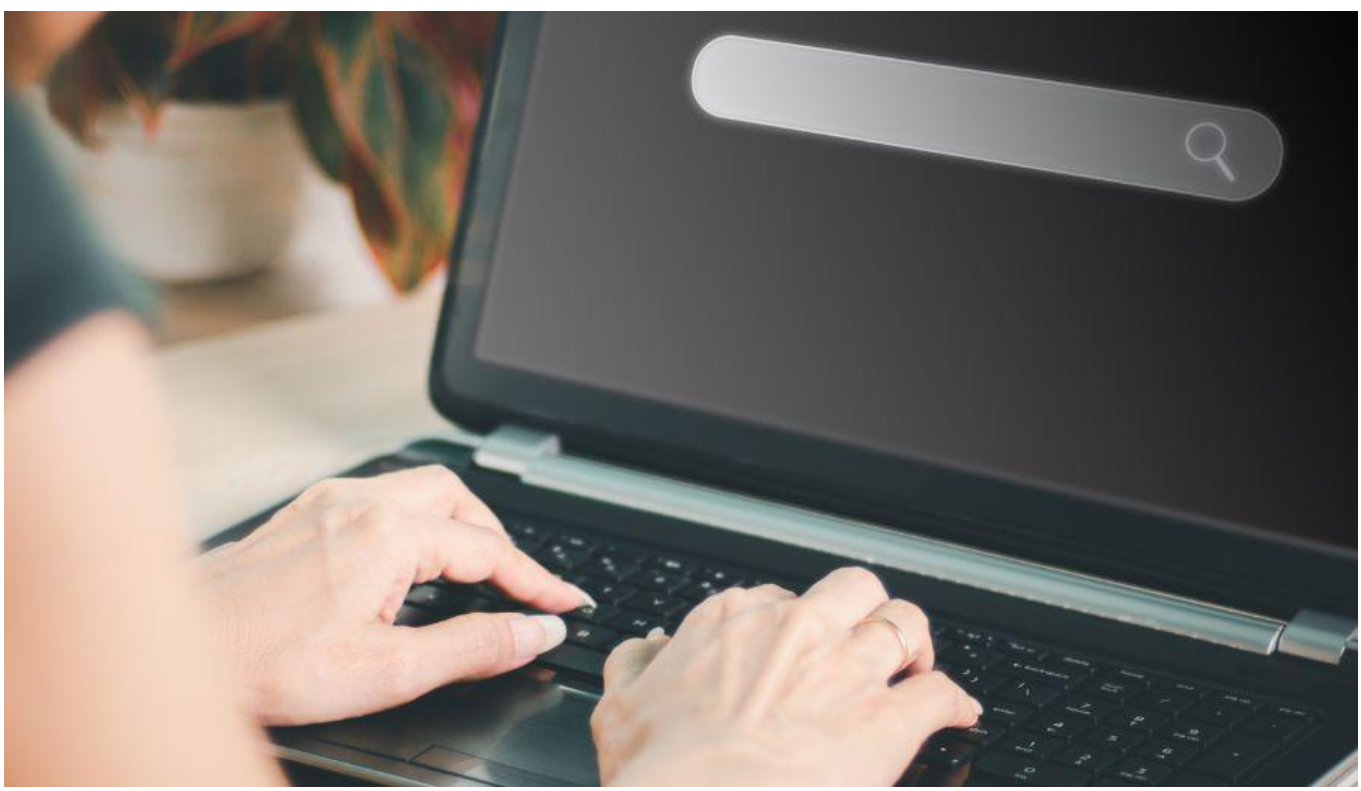


¿Existe alguna forma de conocer qué hacen con nuestros datos en Internet?

Esta pregunta ha ido ganando peso en los últimos años. **La sociedad es cada vez más consciente de los riesgos inherentes a su publicación**. Sin embargo, no debes asustarte y dejar de utilizar Internet. Lo importante es que tengas en cuenta los problemas que pueden surgir y que desarrolles las defensas necesarias.

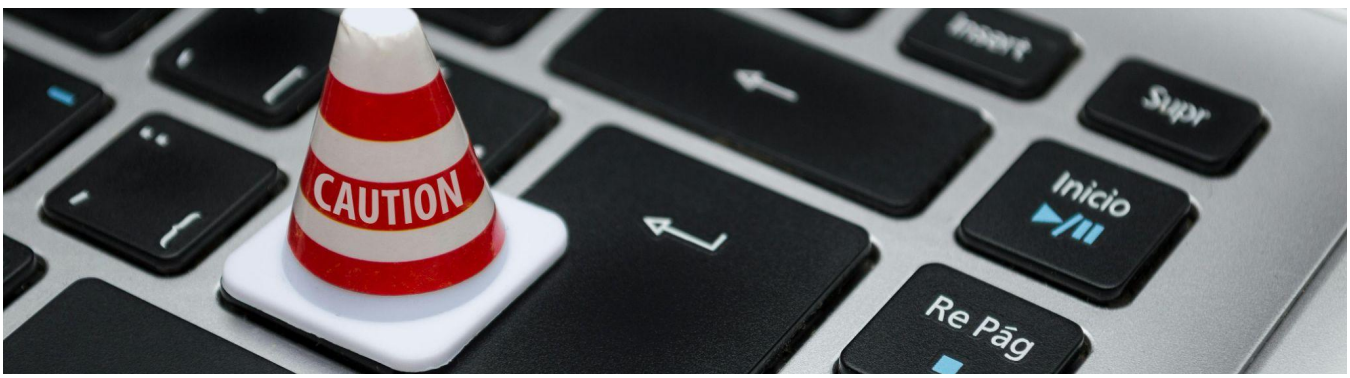
Por suerte, existen varias maneras de comprobar qué información sobre ti está disponible en la red. **Una de ellas es poner tu nombre en un buscador**. De esta manera tan sencilla quizás veas que apareces en diferentes redes sociales, sobre las que puedes ejercer un fuerte control. También es probable que aún existan documentos oficiales donde se muestren tus datos.

Google te permite consultar un resumen de tus datos desde tu propia cuenta. Solo tienes que visitar el panel de control, acceder a «Datos y Privacidad», «Tus datos y opciones de privacidad», luego en «Datos de aplicaciones y servicios que usas» y, por último, clica en «Contenido guardado de servicios de Google». Además, en cada servicio puedes descargarte una copia de la información que contienen.



Otra opción reside en utilizar páginas web destinadas analizar tu rastro en Internet. Una de ellas es Mine, que **es capaz de rastrear qué empresas y servicios tienen datos relacionados contigo**. Además, te permite enviar solicitudes para que los borren, identificar los que más empleas y marcarlos como necesarios. Si bien recurrirá a tu correo electrónico para llevar a cabo su investigación, puedes borrar tu cuenta con facilidad y sin dejar rastro.

También son útiles las **alertas de Google**. Cabe la posibilidad de configurarlas para que te avise cuando aparezca tu nombre, apellidos, correo electrónico, número de teléfono o el DNI. Es una herramienta especialmente útil si has sufrido una suplantación de identidad, ya que te permitirá realizar un rastreo mínimo. Sin embargo, si te encuentras en esta situación, no dejes de ponerte en contacto con la Policía.



La Agencia Española de Protección de Datos (AEPD)

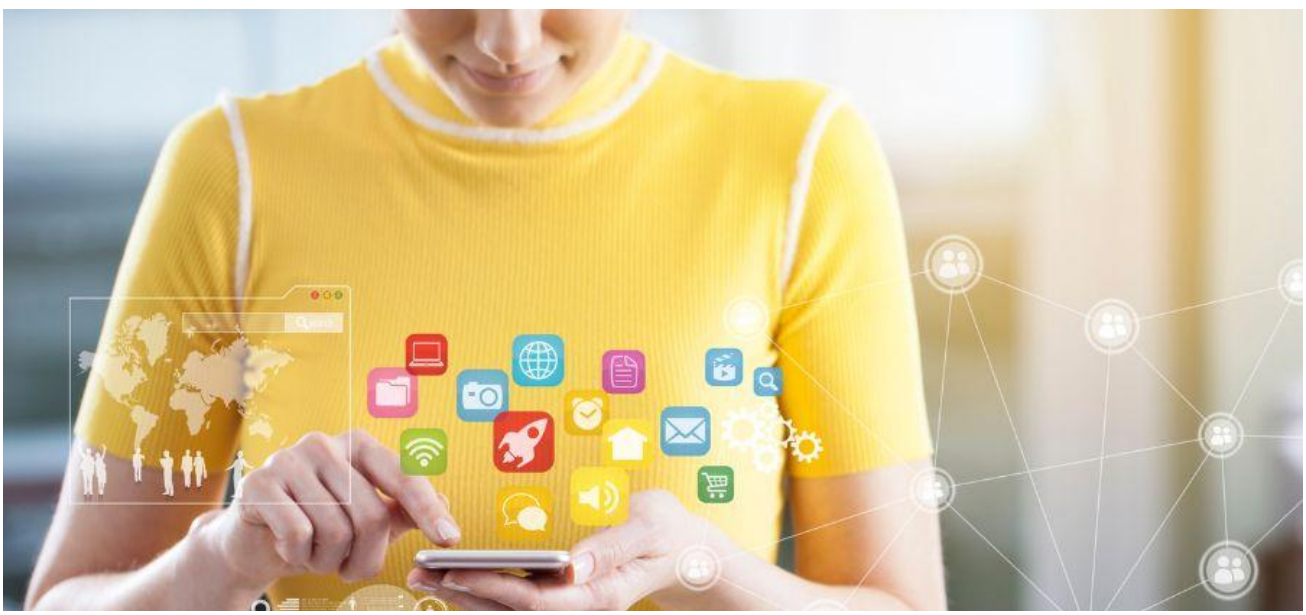
Este organismo público se encarga de **proteger tus derechos de rectificación, oposición, supresión, portabilidad y limitación al tratamiento de decisiones automatizadas**. Si las empresas no responden a tus peticiones de borrado de datos, puedes interponer una reclamación ante la AEPD.

La Agencia dispone de modelos de documentos específicos para ejercitar tus derechos, puedes efectuar las consultas que necesites y tener su apoyo cuando este sea posible. También ofrecen ayuda específica a menores, un grupo de la población especialmente vulnerable a los riesgos que entraña Internet. No dudes en contactarles ante cualquier indicio de problema grave que detectes (acoso en redes sociales, suplantación de identidad, distribución de imágenes o vídeos personales no autorizados, etc.).

A la hora de solicitar su apoyo, es necesario especificar los motivos concretos de la solicitud, ya que **deben existir razones de peso para abrir una investigación**. Si has abierto una reclamación ante una empresa y esta no ha contestado en el plazo previsto en la ley (un mes), la AEPD podrá ayudarte. De esta manera tienes de tu lado una ayuda inestimable para hacer valer tus derechos.

¿Cómo puedes evitar filtraciones de información personal en la red?

Cada persona puede evitar que su información privada, o gran parte de la misma, acabe en Internet sin su consentimiento. **No es necesario que dispongas de conocimientos avanzados para minimizar tu exposición**. Al fin y al cabo, la mayoría de las plataformas disponen de herramientas con las que proteger tu privacidad de forma efectiva.



Para empezar a cuidar tu privacidad, **ten en cuenta las aplicaciones que instalas tanto en tu navegador como en tu teléfono**. Estas suelen pedir datos personales o acceso a áreas concretas del dispositivo. Si no estás de acuerdo con lo que te solicitan, no la instales y busca una alternativa que parezca más segura. Por suerte, existe una amplia variedad de opciones.

Cuando visites cualquier página web, revisa que cumpla con el **RGPD** (Reglamento General de Protección de Datos) y la **LOPD** (Ley Orgánica de Protección de Datos de Carácter Personal), ambas normas de obligado cumplimiento. La página también debe disponer de un aviso legal con los términos y condiciones de la web y contar con una política de *cookies*.

Esta última consiste en una declaración sobre un fragmento de texto que indica los sitios web que visita tu navegador (las *cookies*), y que indica cuáles están activas, qué información rastrean, con qué finalidad y a qué parte del mundo se envía.

Tampoco **dejes de cuidar la privacidad en las redes sociales**. Estas plataformas han cambiado radicalmente la forma en la que la sociedad se relaciona en la red. Además, es muy sencillo dar a conocer una amplia variedad de datos sin que seas consciente, algo a lo que contribuirán tus amistades. Así que, debes mantener diferentes precauciones.

Empieza por dedicar el tiempo necesario a configurar la privacidad de la cuenta. Esto te permite decidir quién ve tus publicaciones, administrar bloqueos, dar privacidad a las fotos, limitar el acceso a las aplicaciones o mantener tu perfil en modo privado. Gracias a estas opciones, y otras específicas de cada plataforma, te ahorrarás problemas con las filtraciones de tu **información personal** o **identidad**.

Además, **asegúrate de que el acceso a los datos de las redes sociales es exclusivamente tuyo**. Esto evitará que tu nombre o alias, contraseña y otras informaciones acaben llegando a terceras personas. Tampoco publiques información personal sensible, como tu número de teléfono o el domicilio en el que resides.

En definitiva, cuidar de tus **datos personales** es posible, aunque necesitas tomar las medidas apropiadas. La amplia mayoría de páginas web cuida la información de sus personas usuarias de acuerdo a la ley. Sin embargo, recuerda que incluso tú puedes dar informaciones accidentalmente de manera directa, por lo que no dejes de tener cuidado.

vuela

1.2

Contraseñas seguras: todo lo que necesitas saber para protegerte

Las contraseñas seguras son la primera línea de defensa al navegar en la red. No importa la plataforma que utilices, siempre tendrás que crear un perfil con un nombre de usuario y una contraseña, que evitará accesos no permitidos. Sin embargo, si el código que has introducido es demasiado simple, corres el riesgo de que sea fácilmente adivinable y el sentido de crear una contraseña se pierda.

En este apartado aprenderás a generar contraseñas sólidas, difíciles de averiguar y que te permitirán disfrutar de una navegación segura en Internet. Pero antes, repasemos cuáles son las técnicas que utilizan los y las ciberdelincuentes para conocer nuestras contraseñas, de este modo seguro que te resulta más sencillo proteger tus perfiles de las filtraciones de seguridad.

Junta de Andalucía

Agencia Digital de Andalucía

Las técnicas que emplea un *hacker*

Obtener las contraseñas es el camino más sencillo para cometer un robo. Un *hacker* (pirata informático) cuenta con una amplia variedad de herramientas y técnicas, que no dudará en poner en marcha. **El objetivo que tienes que perseguir es dificultar e impedir su tarea**. Al igual que proteges una casa con una puerta de seguridad blindada, puedes defender tus cuentas en la red de maneras similares. Sin embargo, veamos cómo asaltan una contraseña.

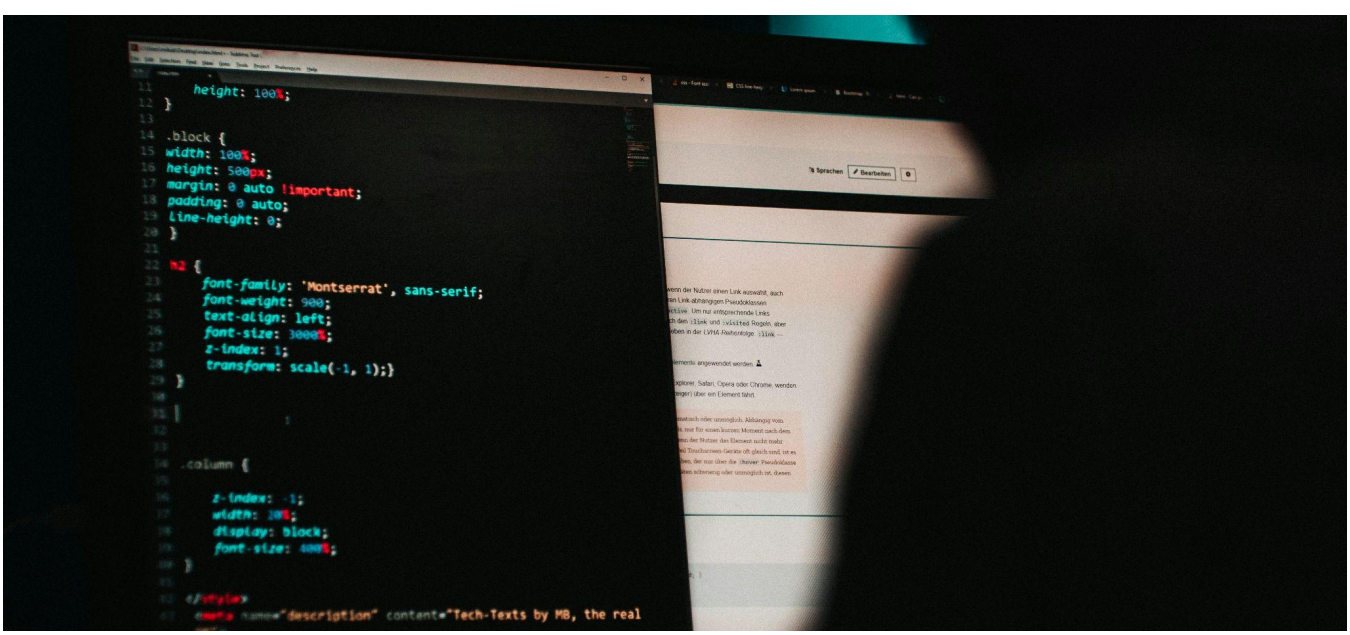
Fuerza bruta

Un **ataque de fuerza bruta** es el más sencillo que pueden poner en marcha. **Consiste en descifrar una contraseña mediante ensayo y error**. La persona que ataca va probando diferentes combinaciones hasta que da con la adecuada. No pienses que este es un trabajo que les llevará mucho tiempo, ya que antes tratan de recabar información sobre su objetivo que les facilite la tarea.

Esto les permite obtener todo tipo de datos personales a través de la **ingeniería social**. Como veremos más adelante, esta técnica normalmente busca ganar la confianza de la persona internauta para conseguir que coopere bajo su manipulación y engaño; por ejemplo, facilitando sus datos personales.

Al final, si logra tener éxito, conseguirá acceso a tu correo electrónico, perfil de una red social o datos sensibles para suplantar tu identidad o tratar de acceder a tus cuentas bancarias.

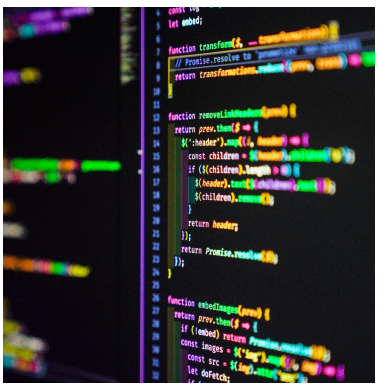
Para protegerte de estos ataques, **es importante crear una contraseña robusta**. Ten en cuenta que cuanto más sencilla sea tu clave, menores dificultades le estás poniendo a quien ataca. Hay personas que llegan a introducir códigos tan simples como 123456, sus propios carnets de identidad o números de teléfono. Así que, aunque la red es, por lo general, un lugar seguro, debes poner de tu parte para reforzar la protección a la hora de navegar.

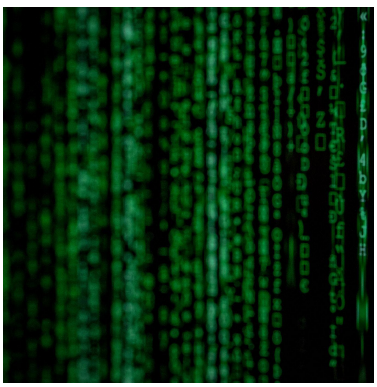


Ataque por diccionario

En este caso, las personas que delinquen usan un programa para realizar el ataque. Este **actúa de forma autónoma y ejecuta diferentes comprobaciones de letras**. Empiezan por combinaciones sencillas hasta llegar a las más complejas. Es una técnica efectiva, que les llevará tiempo pero que terminará por encontrar el código adecuado. Su eficacia es mayor que la de un ataque de fuerza bruta.

Además, **el programa también utiliza palabras de diccionario**. Muchas personas recurren a palabras concretas para crear sus contraseñas (nube, perro, vaca…), por lo que tarde o temprano encontrará la adecuada. Por esta razón es recomendable que combines cifras, letras, mayúsculas, minúsculas y símbolos. Este tipo de ataque perderá gran parte de su efectividad, ya que no podrá encontrar el término adecuado con facilidad.





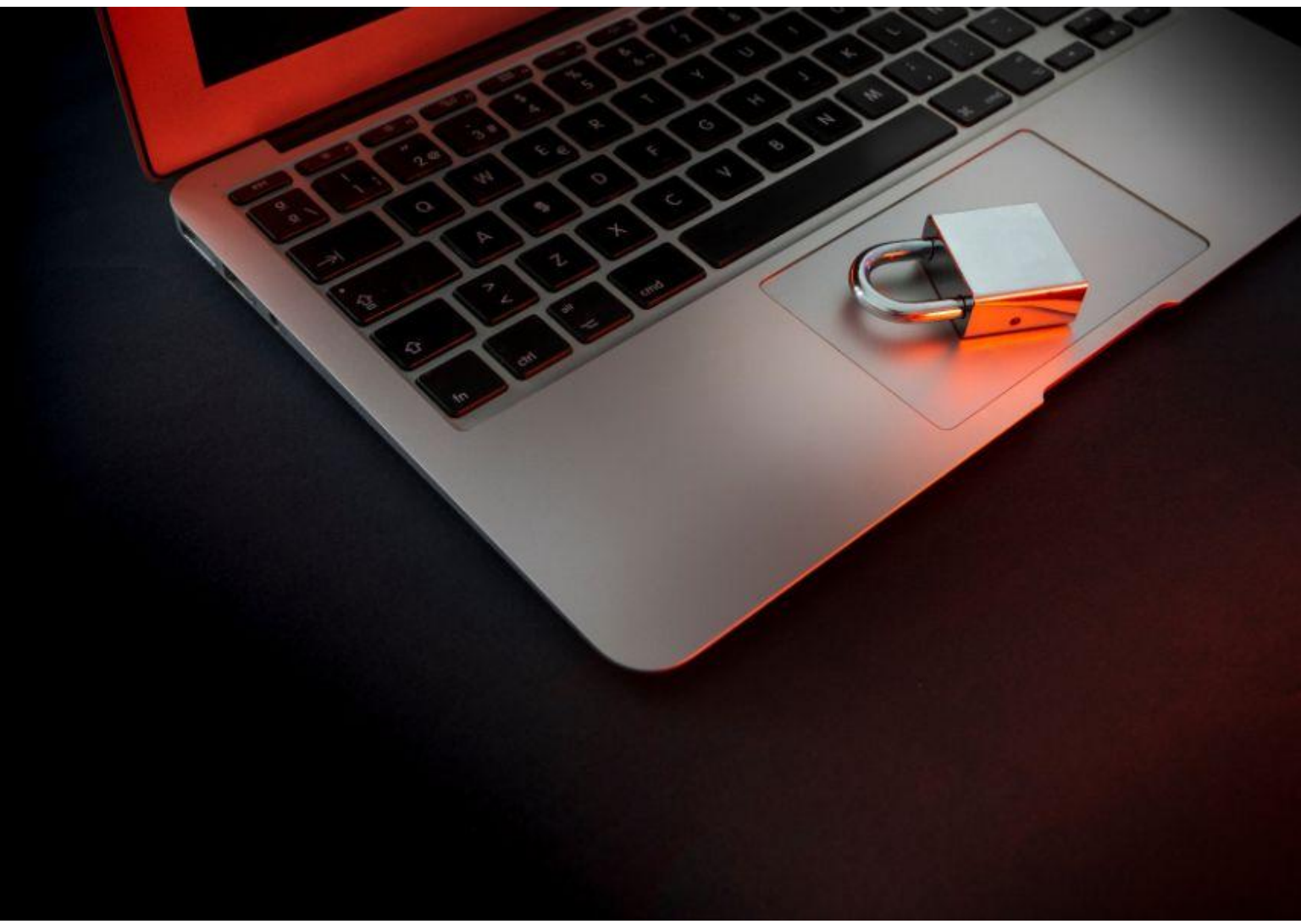
Ataques que emplean ingeniería social

Los ataques con **ingeniería social** recurren a técnicas dirigidas a las personas. **Tienen como objetivo conseguir información personal suficientemente relevante como para controlar tus dispositivos**, por poner un ejemplo. La manipulación o el engaño son métodos usados con frecuencia. Asimismo, suelen ser el paso previo al envío de programas maliciosos.

Existen varias técnicas dentro de este tipo de ataques, la mayoría tienen nombres en inglés. Por ejemplo, **mediante el *phishing* tratarán de obtener información personal importante a través de tu correo electrónico o redes sociales**. Por otra parte, el *vishing* se lleva a cabo mediante llamadas de teléfono, o el *smishing* vía mensaje de texto (SMS). En todos ellos, la persona atacante suplanta la identidad de una entidad legítima, como tu comercializadora de electricidad, y te pide datos personales.

Por otro lado, **el uso de ganchos o cebos es otro tipo de ataque de ingeniería social**. En este caso, quien ataca recurre a un cebo que está diseñado para llamar la atención y despertar tu curiosidad. Por ejemplo, ofrecer un producto gratis. El objetivo es propagar y ejecutar programas maliciosos, que accederán a tus datos personales y los robarán. También pueden tratar de tomar el control de un dispositivo o propagarse por una red.

Por último, el *spam* es una de las técnicas más conocidas. **Se trata del envío masivo de correos electrónicos sin que los solicites**. Por regla general, acaban en la bandeja de mensajes no deseados de tu correo, aunque algunos acceden a la principal (donde sueles recibir tus correos normalmente) y tendrás que borrar. La finalidad es la de maximizar las oportunidades de éxito de ataques tipo *phishing* o infectar tu dispositivo con programas maliciosos.



¿Cómo defenderte de los ataques?

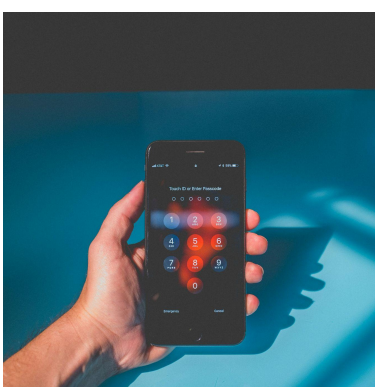
Por lo general, la red es segura, pero eso no significa que no debas tener una serie de precauciones a la hora de navegar. Ahora que conoces los principales ataques que puedes sufrir, llega el momento de descubrir cómo defenderte. Si tomas las medidas oportunas, tu contraseña estará más protegida ante las posibles amenazas.

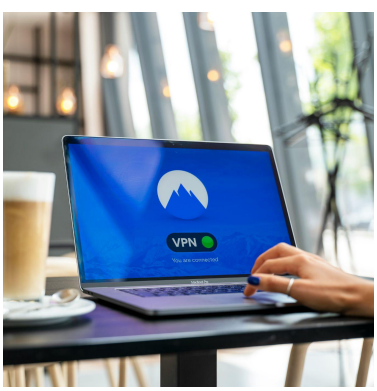
Defensa ante ataques de fuerza bruta y de diccionario

La forma más sencilla de defenderte es contar con contraseñas robustas. Además, **siempre que sea posible, recurre a factores de autenticación múltiple**. Se trata de sistemas que utilizan tanto contraseñas como otros métodos de identificación, para evitar intrusiones en tus perfiles. Los bancos son un buen ejemplo, ya que combinan el uso de contraseña con envíos de códigos a tu teléfono móvil. De esta manera, las probabilidades de accesos indebidos se reducen al mínimo.

Procura que las contraseñas que emplees tengan más de 10 caracteres. Si la persona atacante cuenta con medios básicos para realizar el asalto, tardará una semana o más en completarlo. Este tiempo acabará por disuadirle del intento, ya que tanto esfuerzo no merecerá la pena. Por esto es importante combinar números con letras, mayúsculas, minúsculas y símbolos. Gracias a ellos, los algoritmos de los programas para efectuar ataques serán menos efectivos.

Una buena forma de crear una contraseña segura es usar una frase que tenga un significado especial para ti, y preferiblemente, para nadie más. Esta debe ser de cierta longitud para dificultar su adivinación, pero tampoco muy larga para recordarla con facilidad. Ejemplo: «En el bar de Ana venden bocadillos enormes a 4 euros». Ahora, selecciona la primera letra de cada palabra y tu contraseña resultante será «EebdAvbea4€». Si no se te ocurre nada, siempre puedes recurrir como punto de partida a alguna cita célebre que te guste o a tu canción favorita, por citar dos ideas.





Protegerte frente a la ingeniería social

La protección frente a estos ataques puede llegar a ser más compleja que en los casos anteriores. Al fin y al cabo, se centran en el engaño y en resultar atractivos. Para empezar, **la precaución es la clave para evitar problemas a largo plazo**. Si recibes un correo electrónico con peticiones urgentes como por ejemplo «Oferta exclusiva para ti solo en las próximas 24 horas» o «Tienes un paquete pendiente de entrega. Reclámalo si no quieres perderlo», lo mejor es que no le prestes atención.

Los mensajes que te envíen contendrán, en la mayoría de los casos, **errores gramaticales o combinaciones de palabras que no tienen sentido**. Además, revisa el remitente del correo para comprobar si se trata de la organización que dice ser. Así, te aseguras de la legitimidad de la información que contiene el mensaje.

No descargues ningún archivo adjunto y, si lo recibes en tu teléfono móvil o *tablet*, no cedas el control de ningún área del dispositivo. En estos casos, es necesaria la precaución como forma de evitar daños graves. Ten en cuenta que buena parte de los problemas de ciberseguridad son de origen humano. Es por esto que la **ingeniería social** es un método de ataque tan efectivo.

Errores a evitar cuando creas una contraseña

Las contraseñas robadas que más riesgo entrañan son aquellas que se reutilizan una y otra vez. Esto ocurre cuando usas el mismo código para varios perfiles o plataformas. De este modo, solo simplificas los ataques. Si estás en el punto de mira de un delincuente, este conseguirá el acceso a tus cuentas en cualquier lugar. Procura que sean específicas y apúntalas en un documento electrónico o en una libreta para no olvidarlas.

Bajo ningún concepto compartas tus contraseñas en la red, salvo con personas de total confianza y a través de canales cifrados. Un ejemplo frecuente es la tendencia a compartir los códigos de una plataforma de *streaming*. Llegará un momento en el que no tendrás control sobre la propia cuenta, lo que aumenta el riesgo de que se produzca un robo.

Emplear expresiones hechas o conceptos simples no es una buena idea para crear una contraseña robusta, ya que es posible adivinar contraseñas mediante un ataque de diccionario (un método que prueba todas las palabras del diccionario para adivinar la contraseña). Tampoco recurras a datos personales como tus aficiones, DNI o número de teléfono. Suelen estar entre las primeras opciones de intento de adivinación.

Por otro lado, y aunque te parezca lo contrario, **cambiar continuamente las contraseñas no es una buena idea**. Es recomendable modificarlas cada cierto tiempo, como a los seis meses o al año, pero hacerlo más frecuentemente te traerá problemas. Te costará recordarlas, olvidarás apuntar alguna o el código usado será cada vez más simple.

En definitiva, las **contraseñas seguras** son cruciales para garantizar tu seguridad en la red. Es necesario que generes códigos robustos que dificulten el acceso a tus perfiles. Recuerda que para disfrutar de todas las oportunidades que ofrece Internet de forma segura solo tienes que seguir las sencillas pautas que te hemos explicado.

vuela

1.3

Malware. Qué es y cómo puedes prevenirlo de forma muy efectiva

Navegar por Internet y usar las tecnologías digitales puede facilitarte numerosas oportunidades en todos los aspectos de tu vida: la escuela, el trabajo, el tiempo de ocio, etc. No obstante, para disfrutar plenamente de estos beneficios te recomendamos que integres en tu comportamiento digital una serie de pautas de ciberseguridad para combatir riesgos como el *malware*. ¡Verás que sencillas!

En este apartado conocerás los principales tipos, así como los mejores consejos para identificarlos.

Junta de Andalucía

Agencia Digital de Andalucía

Los principales tipos de *malware* a los que debes prestar atención

Un *malware* es un *software* que se infiltra en tu ordenador con alguna intención maliciosa. Su propósito puede ser muy diverso, es por eso que, para facilitar que puedas detectarlos rápidamente, hemos creado una lista con los seis principales tipos de *malware* y sus características.

1. Virus informático

El **virus es, a buen seguro, uno de los *malware* que más te sonará**. La meta principal que persigue es alterar el funcionamiento de tu ordenador. Sin embargo, una de las principales ventajas que tienes a tu disposición es que no puede actuar sin tu intervención.

En este sentido, **son totalmente visibles y viajan por tu ordenador** a través de archivos ejecutables (es decir, que les puedes hacer clic). Los podrás identificar porque acaban en .exe. Sin embargo, tienen el nombre de una aplicación falsa para engañarte y que los abras. Es importante, en este sentido, que solo abras ficheros de fuentes confiables para evitar este tipo de contratiempos y que cuides las descargas, permitiendo solo aquellas que proceden de sitios web seguros.

2. Gusano informático

El **funcionamiento del gusano informático** es **similar al de un virus**, aunque con un pequeño matiz. No requiere tu intervención, ni tampoco la modificación de un archivo en concreto. Tiene la capacidad de expandirse por tu ordenador y llegar a tu lista de contactos. De esta forma, a través de tu base de datos, puede reproducirse y llegar a otros equipos.

Este tipo tiene una mayor complejidad a la hora de que lo puedas detectar. No afecta al funcionamiento general del equipo, aunque sí consigue que algunas tareas rutinarias que llevabas a cabo se vuelvan más lentas. El lado positivo es que prácticamente todos los antivirus protegen ante este tipo de *malware.*

3. Troyano

¿Conoces la historia del caballo de Troya que aparece en la Odisea de Homero? Tras años de batalla, los griegos no consiguieron sobrepasar los altos muros de la ciudad troyana hasta que se decidió **llevar a cabo un plan de engaño**: entrar camuflados dentro de un caballo de madera.

En este caso, **el troyano** actúa de una forma similar. Al ejecutar un archivo que piensas que es legítimo, este en realidad es un **troyano**. De esta forma, es capaz de robar parte de tu información confidencial. Igual que en el caso anterior, con un buen antivirus actualizado tus dispositivos contarán con protección frente a este tipo de ataques.

4. *Spyware*

El objetivo del ***spyware***, en este caso, es recolectar información personal de tu ordenador que sea sensible sin tu autorización. No hace falta tu intervención para su instalación, ya que este *software* malicioso puede hacerlo por sí solo. Actúa sin dejar rastro, por lo que podrás seguir llevando a cabo todas tus actividades rutinarias en el equipo.

Sin embargo, **el *spyware* es capaz de monitorizar** y recopilar todos los datos que encuentre en tu ordenador y en tu disco duro. Asimismo, tiene acceso a tu historial de navegación en Internet y a todas las aplicaciones que haya podido instalar. Por otro lado, tiene la capacidad de añadir sus propias aplicaciones.

5. *Adware*

A diferencia de **otros tipos de *software* malicioso**, éste aparece a través de la publicidad. Cuando navegas por Internet, en algunos sitios web puedes encontrarte con diferentes tipos de ventanas emergentes que no te dejan en paz. Intentas cerrarlas, pero siguen apareciendo. Por suerte, solo se encuentran en una pequeña parte de los sitios web.

Puedes confundirlo solo con publicidad no deseada, pero puede llegar a captar tus datos personales. Por esta razón, **los expertos alertan del *adware***.

6. *Ransomware*

Es una de las **metodologías de *phishing*** más habituales en los últimos tiempos. ¿Qué significa esto? Básicamente, las y los ciberdelincuentes se hacen pasar por una de tus fuentes confiables. Es un tipo de amenaza muy enfocada a las empresas ya que su pauta de actuación es el secuestro de datos, por el que pedirán un rescate económico posteriormente.

Al abrir uno de sus correos electrónicos, son capaces de ingresar el *software*. Posteriormente, te aparecerá un mensaje en la pantalla informándote del ataque. **Podrás pagar el rescate a través de SMS, PayPal o bien criptomonedas**. Por suerte, son uno de los más fáciles de prevenir, ya que solo debes estar alerta a la hora de abrir los mensajes que lleguen a tu bandeja de entrada de correo electrónico.

Cómo identificarlos fácilmente

Una vez ya conoces **los principales tipos de *software* malicioso**, es fundamental que conozcas las formas de identificarlos rápidamente. Además, queremos darte algunos consejos para que puedas **conseguir la protección** para tu equipo de todas las amenazas que puedes encontrar en Internet. De esta forma, navegarás sin preocupaciones.

Una de las primeras señales de alerta es un rendimiento lento del equipo. Puede deberse a muchas razones, como **la falta de espacio en el disco duro o una memoria RAM limitada**, por lo que es importante que tomes con precaución esta hipótesis y sigas investigando. También hay que prestar atención a si tu equipo tiene problemas tanto para encenderse como para apagarse.

Internet también puede darte algo de luz acerca de si tu equipo está infectado por un *software* malicioso. En el caso de que quieras ir a un sitio web y **acabes yendo a otro totalmente diferente con asiduidad puedes indicar una señal de peligro**. Lo mismo en el caso de que te aparezcan más anuncios emergentes de lo habitual, o te salgan mensajes de que tu equipo está infectado y te intenten vender antivirus.

Estas son algunas de las principales alertas, pero es importante que tengas claro cómo protegerte para que puedas acabar con todas estas amenazas.

Principales medidas contra *softwares* maliciosos

Una de las primeras prácticas que debes incluir a la hora de navegar por Internet es confiar solo y exclusivamente en aquellas fuentes que sean fiables. En este sentido, a la hora de descargar programas, no lo hagas de sitios web de los que desconfíes.

Lo mismo ocurre con la bandeja de entrada de correo electrónico. Solo abre correos de aquellas personas que sean de confianza. Sobre todo, debes desconfiar de hacer clic en enlaces comerciales, si no vienen de fuentes que hayas solicitado. Esta es la primera medida para **prevenir tu ordenador adecuadamente contra un *software* malicioso**.

En otro orden, debes aplicar la misma lógica con los anuncios que veas en Internet, y, sobre todo, con aquellos que tengan ofertas comerciales dudosas. Es importante que tengas guardados en lugares seguros todos tus datos sensibles como **las claves de acceso a tu cuenta bancaria *online***. Cuando el ordenador te ofrezca guardar contraseñas, dile que no, ya que en caso contrario tendrías la clave en el equipo y podría ser robada por un ataque malicioso.

Todos tus datos más importantes **deben ser guardados en una copia de seguridad**. De esta forma, si tu ordenador se infecta y necesitas restablecerlo de cero podrás mantener todos los archivos y ficheros que puedas necesitar. Para ello, en tu PC deberás ir al panel de control y seleccionar la opción de sistema y mantenimiento.

Posteriormente, selecciona copia de seguridad y restauración. Elegirás la opción de crear una imagen del sistema y deberás seguir los pasos que te indique el asistente de instalación. En el caso de que te soliciten una contraseña de administrador, deberás ponerla.

Contar con un *antimalware* también te ayudará a prevenir y tener tu equipo bien protegido. Uno de los más recomendables es **Avast**. Actualmente, ya **está presente en aproximadamente el 40% de los equipos del mundo**. Encontrarás una versión totalmente gratuita, y además es accesible.

Lleva a cabo revisiones de tu ordenador de forma automática, y cuenta con un sistema de notificaciones claro. Te da toda la información que necesitas para actuar en consecuencia. Si tu sistema operativo es Windows puedes recurrir directamente al antivirus que viene instalado en tu ordenador, Windows Defender.

Otra de las opciones, **especialmente para pymes, es malwarebytes**. Sirve tanto para empresas como para particulares. De forma gratuita, ofrece un escaneo de tu equipo para conocer su estado y saber si está infectado.

Como conclusión, la aplicación de este manual de buenas prácticas te permitirá **acabar con los *malware* rápidamente** y navegarás por Internet de una forma totalmente segura.

vuela

1.4

Software malicioso: ¿Qué es y qué deberías hacer para evitarlo?

Navegar de forma segura por Internet requiere conocer los riesgos y saber detectarlos. Tú también puedes contribuir a hacer de Internet un lugar mucho más seguro para todos y todas. Por ello, vamos a explicarte de manera sencilla qué es **un *software* malicioso** y qué puedes hacer para evitar que entre en tus dispositivos.

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es un *software* malicioso?

Todos los días entra una gran cantidad de datos a tus dispositivos, como el ordenador o el *smartphone*. Descargas de archivos, transferencias de datos y mensajes recibidos quedan almacenados en su interior. Incluso si los eliminas, siempre quedará una huella en los registros más ocultos. Por suerte, puedes controlar lo que entra y lo que no.

Antes de aclarar este aspecto, debes saber qué es un *software* en sí. Para explicártelo brevemente, te daremos a conocer dos conceptos que muchas veces se tienden a confundir:

- Un ***software*** es un programa o aplicación que realiza una determinada función en tu dispositivo.
- Un ***hardware*** es la parte física, es decir, el ordenador, el teléfono móvil o cualquier otro soporte.

Respecto al primero, abarca gran cantidad de archivos de diferentes tipos. Todos tienen en común que permiten a tu aparato ejecutar una determinada tarea. Lo que tienes que saber, básicamente, es que los *softwares* son imprescindibles para que puedas utilizar tus dispositivos. Sin ellos, sería totalmente imposible.

Ahora bien, un *software* malicioso (también llamado *malware*) es un programa o conjunto de datos creado por un ciberdelincuente. Sus objetivos pueden ser muy diversos, pero destacamos los siguientes:

- **Robar datos**: Es muy habitual que infecten tu ordenador para conseguir tus datos personales. Información como contraseñas de acceso o cuentas bancarias son el objetivo que persiguen.
- **Corromper archivos**: Esto sucede sobre todo en los ordenadores de empresas y entidades. A veces, se busca detener su funcionamiento o averiarlo para hacer caer a todo el sistema informático.
- **Suplantar la identidad**: Las y los ciberdelincuentes roban datos personales para hacerse pasar por sus víctimas. De esta manera, pueden realizar sus estafas bajo otra identidad.

A pesar de todo lo anterior, no debes alarmarte. Internet puede ser un lugar muy seguro si tomas las debidas precauciones. Afortunadamente, **tienes muchos programas y consejos de protección a tu disposición** para evitar que este tipo de virus entre a tu sistema.

¿Dónde puedes encontrar *software* malicioso?

Navegar por la red es como ir por una ciudad: lo importante es que sepas a dónde vas. Si tienes el control de tu interacción respecto al mundo *online*, sabrás elegir entornos seguros y descartar aquellos que no lo son. Hacer esto requiere, obviamente, conocer una serie de prácticas que no debes llevar a cabo.

En descargas

Cuando descargas un archivo por Internet, estás permitiendo que los datos creados por otra persona entren en tu dispositivo. Hay páginas en las que es recomendable descargar, como en las páginas oficiales o las páginas de desarrolladores de programas. Sin embargo, **los sitios web que ofrecen descarga de música o películas, además de ser ilegales, son peligrosos**.

Por correo electrónico

¿Qué haces cuando recibes un correo electrónico de un remitente desconocido? Muchas veces, lo abrimos y consultamos lo que contiene. Otras personas se atreven a clicar en los enlaces que encuentran. Nunca debes hacer esto, ya que a veces redirigen a una página de descarga para infectar tu dispositivo.

Con archivos adjuntos

Si recibes un SMS o un mensaje en tus redes sociales con archivos adjuntos y no conoces al remitente, desconfía. En ocasiones, pueden contener un texto llamativo con un enlace. Al clicar en este, accedes nuevamente a una página de descarga y abres la puerta a tu ordenador o teléfono móvil a posibles amenazas.

¿Qué tipos de *malware* existen?

El conocimiento es la base de la seguridad. Por ello, **es fundamental que aprendas a identificar los *malware*** que pueden infectar tu ordenador. Existen múltiples tipos de *software malicioso*, pero estos son los que más debes conocer.

1. Virus

Son los más conocidos. Se trata de programas configurados para hacer una determinada acción en tu ordenador. Sus consecuencias son muy diversas, aunque las más comunes incluyen robo de datos o corrupción de archivos.

2. Troyano

Es un tipo de *malware* que **funciona sin que te des cuenta**. Mientras lo hace, deja la puerta abierta para que otros virus puedan entrar y continuar agravando el problema.

3. Gusano

En este caso, los virus pueden entrar en tu lista de dispositivos conectados para **replicarse hacia ellos**. Una vez que han entrado en varios sistemas, se activan a la misma vez para realizar una determinada acción.

4. Spyware

Se instala y activa sin tu conocimiento para recabar datos e información personal. Algunos sistemas sofisticados pueden hacerlo rastreando el orden de las teclas que pulsas para averiguar las contraseñas.

¿Cómo sé si mi equipo está infectado con *malware*?

Los principales síntomas para detectar si están presentes en tu equipo son los siguientes:

- Te aparecen **mensajes emergentes** constantemente o publicidad cuando no estás navegando por Internet.
- La velocidad se reduce considerablemente sin razón aparente o se bloquea con gran facilidad.
- Te deniega el permiso para llevar a cabo acciones o tareas que siempre has podido efectuar con normalidad.
- **No puedes guardar nuevos archivos** o modificar los datos de los existentes.
- El dispositivo se reinicia sin que se lo ordenes o se pierden los datos guardados.
- Recibes demasiados mensajes no deseados en tu correo electrónico o SMS con publicidad fraudulenta.

Hasta hace varios años, era muy fácil saber si había un *malware* en el ordenador. Sin embargo, su sofisticación ha hecho que ahora puedan actuar sin ser descubiertos fácilmente. Con los móviles sucede algo parecido: antiguamente, no tenían Internet, por lo que no eran susceptibles de recibir contenido malicioso. La progresiva implantación de las tecnologías en nuestra vida diaria requiere que todos y todas hagamos un uso responsable.

Todo lo anterior son síntomas de que tu equipo tiene algún tipo de *malware*. Sin embargo, **la mejor forma de saberlo con seguridad es utilizando un antivirus**. De esta manera, tienes la posibilidad de escanear automáticamente todos los archivos de tus dispositivos y detectar si hay contenido malicioso.

¿De qué forma puedo evitar el *malware*?

Afortunadamente, puedes evitar que este tipo de *software* entre a tu dispositivo si tomas las precauciones adecuadas. A continuación te mostramos varias acciones que debes poner en práctica para que tu navegación por Internet sea cómoda y segura.

1. Cuidado con las descargas

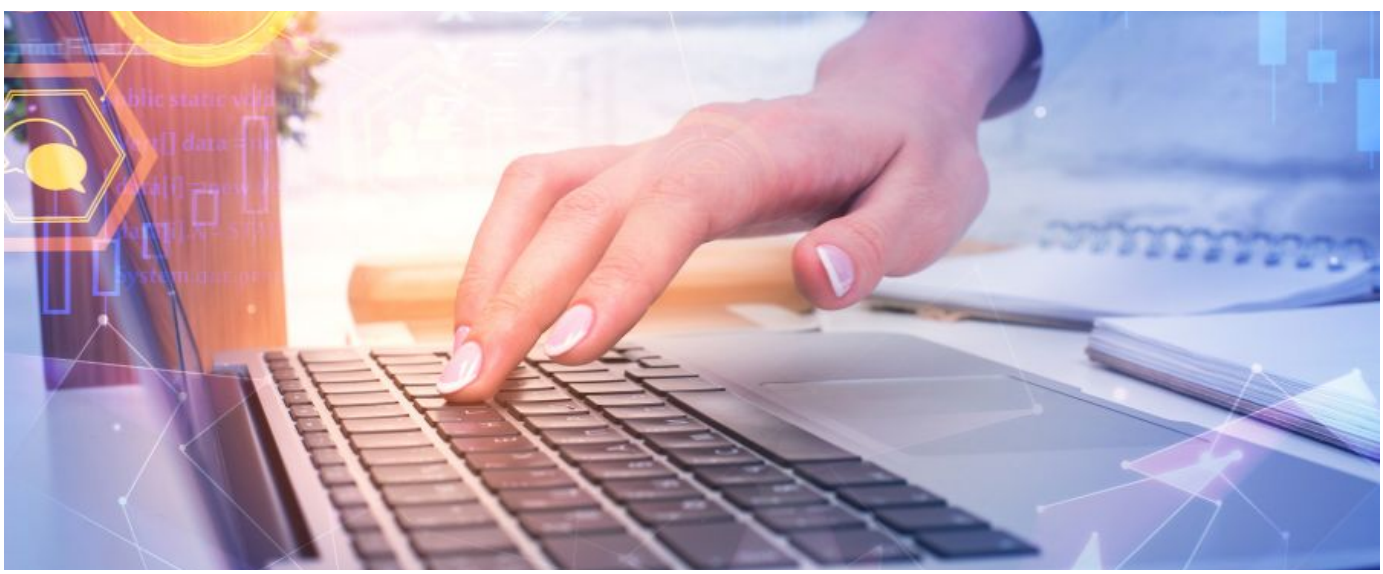
Como avanzábamos antes, esta es una de las principales puertas de entrada de los virus. Evita los portales de descarga de música, películas o similares (recuerda que están prohibidos) y compra el contenido en webs oficiales. En tu teléfono móvil, opta por fuentes oficiales de descarga para los juegos y *apps*.

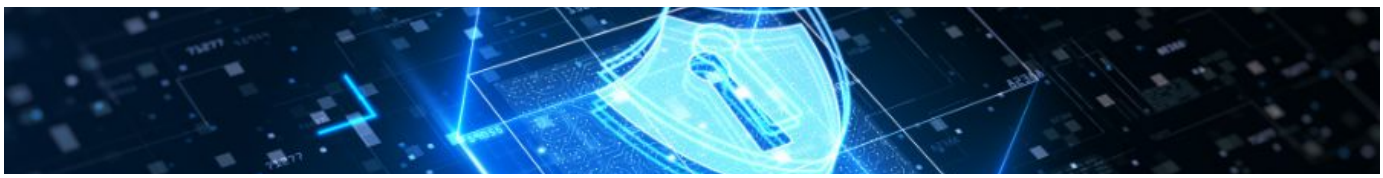
2. Instala un antivirus

Este consejo es básico para un uso seguro de Internet. **Necesitas tener siempre un antivirus con antimalware en funcionamiento** y debe estar actualizado a su última versión. Además, es necesario que realices análisis, al menos, una vez a la semana. La prevención es la mejor solución para combatir los ataques informáticos.

3. Revisa las extensiones de Google

Cuando navegues por la red, no confíes en aquellas páginas que te pidan instalar una extensión. Es muy común que te aparezca un mensaje flotante para que otorgues tu permiso. También te indicarán la necesidad de instalar un determinado programa para continuar en la web. Sea cual sea el caso, desconfía.





4. Actualiza tu sistema operativo

Frecuentemente, recibimos avisos de que es necesario actualizar el sistema principal de nuestro ordenador o teléfono móvil. **La mayoría de las veces los acabamos ignorando, lo que resulta totalmente contraproducente**. Es esencial que lo mantengas siempre en su última versión, ya que es la forma que tienen los equipos de desarrollo de mejorar la seguridad de tus aparatos digitales.

5. Evita las redes públicas dudosas

Cuando te conectes a una red pública, debes tener en cuenta que estás compartiendo espacio con otras personas que no conoces. Por tanto, utiliza solo conexiones de WiFi público seguras. Las podrás detectar por tener un protocolo de seguridad WPA-2 (puedes consultarlo en las propiedades de cada red).

6. Navega por páginas web seguras

El principal peligro para tus dispositivos son las páginas web fraudulentas. Un buen método (aunque no infalible) para saber si una red es segura es fijarse en que tenga estos tres elementos:

- El icono de un candado al lado del enlace (una vez que hayas entrado).
- La denominación «https» (no «http») justo al comienzo del vínculo.
- El aviso legal, que es la identificación obligatoria del propietario de la web (suele aparecer en la zona inferior).

7. Cuidado con los *bots*

En redes sociales, los *bots* son cuentas que simulan ser personas conocidas por ti. Para ello, roban su foto de perfil, biografía y nombre. Después, te envían una solicitud de amistad y un mensaje con contenido infeccioso. Ante la duda, nunca aceptes una solicitud de alguien que no conozcas. Si aparentemente es un amigo o amiga, pregúntale directamente (nunca por la red social).

Si todos y todas contribuimos, **conseguiremos que el *software* malicioso no tenga cabida en nuestros sistemas**.

vuela

1.5

¿Cómo detectar una red WiFi pública segura y cómo navegar en ella?

La tecnología WiFi es un sistema de conexión a Internet sin cable. De este modo, puedes navegar a alta velocidad al encontrarte cerca de un módem o *router*. Probablemente, disfrutes de este avance en tu casa, pero vamos a centrar nuestra atención en la **red WiFi pública**. ¿Sueles conectarte a ella? ¿Sabes cómo hacerlo con seguridad?

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué son las redes WiFi públicas?

Las redes WiFi públicas son los **sistemas de conexión que están disponibles, básicamente, en espacios de libre tránsito**. Por ejemplo, las que se encuentran en negocios de restauración, hoteles y centros comerciales. También entran dentro de esta categoría las que ofrecen las instituciones en las sedes o en la calle para uso ciudadano.

Debes saber que hay dos tipos de WiFi público:

1. Las que no necesitan contraseña de acceso. Generalmente están disponibles en las calles o en centros comerciales.
2. Las que sí necesitan contraseña de acceso y donde se conecta bastante gente, como cafeterías o universidades, por citar dos ejemplos.

Es importante que tengas en cuenta el segundo punto. Una red que requiera contraseña o un simple registro **puede ser considerada pública si un gran número de personas se conecta**. ¿Por qué motivo? Principalmente, debido a que estás compartiendo un entorno *online* con más gente de la que no conoces sus intenciones.

A su vez, una WiFi pública no tiene por qué ser gratuita. Muchos hoteles, por ejemplo, disponen de un sistema de pago por día para sus huéspedes. En estas situaciones, tampoco hay que olvidar que estamos expuestos y expuestas a sufrir algún robo de información en nuestros dispositivos, por lo que debemos actuar con cuidado.

Riesgos de utilizar una red WiFi pública no segura

Como ya avanzábamos, al utilizar una red pública, estás compartiendo un entorno con más personas. Es aquí donde radica el principal riesgo de esta práctica tan normal en nuestra vida diaria. Sin embargo, hay otros riesgos detrás de esto que debes conocer. Obviamente, nos referimos a las redes no seguras, nunca a las que tengan adecuados niveles de protección.

1. Comprueba que la red WiFi pública es real

Puede sonar extraño, pero **el principal riesgo de las redes públicas es que, a veces, ni siquiera existen**. Vamos a explicarlo con un ejemplo: llegas a un restaurante y detectas un WiFi con el nombre del local. Sin dudarlo, te conectas con tu teléfono móvil y empiezas a navegar. Pero ¿y si el negocio no tiene red?

Si la pregunta anterior es negativa, puede que hayas caído en la trampa de alguien que viva cerca. Muchas veces, las personas ciberdelincuentes cambian el nombre de su red para captar dispositivos. Después, roban la información personal y llevan a cabo otras prácticas que afectan a nuestros intereses.

2. Protégete frente al robo de datos

Cuando una persona con malas intenciones puede acceder a nuestro teléfono, le estamos dando acceso a una gran cantidad de información personal. Entre ellas, puede haber fotos, vídeos, mensajes recibidos y enviados, correos electrónicos, contraseñas de redes sociales, aplicaciones, etc.

Para cualquier *hacker* (ciberdelincuente) resulta bastante fácil. Solo tiene que entrar a los archivos de nuestro teléfono para acceder a todo lo que desee. Además, muchas veces pueden copiar nuestros datos más importantes o, simplemente, robarlos. En cualquier caso, supone una grave pérdida de privacidad que debes evitar.

3. Infección con virus

Otro de los peligros que podemos sufrir es recibir archivos maliciosos en nuestro ordenador o teléfono móvil. ¿Qué significa esto? Que otra persona puede infectar nuestros dispositivos con un virus rápidamente. En este caso, las consecuencias pueden ser muy variadas, pero destacan las siguientes:

- Robo de datos para extorsión o suplantación de identidad.
- **Secuestro del dispositivo** para exigir un pago económico.
- Pérdida completa de control del teléfono móvil o del ordenador.

4. Problemas legales

Es muy común confundir una red pública con una red sin contraseña, por eso dividimos las dos categorías anteriormente. Sin embargo, el problema surge cuando nos conectamos a un WiFi privado pensando que pertenece al local en el que nos estamos tomando un café.

En España, conectarse a una red privada sin autorización (popularmente denominado «robo de WiFi») está prohibido. Dependiendo de la gravedad, las multas podrían ser más o menos cuantiosas. De todos modos, cabe tener cuidado y saber siempre a dónde nos estamos conectando.

¿Cómo identificar una conexión WiFi segura?

Hay varias claves que pueden ayudarte a **identificar una conexión WiFi segura**. Ante todo, recuerda: **si no tienes certeza sobre si la red es fiable, no te conectes**.

Averiguar el protocolo de seguridad

El protocolo de seguridad de redes WiFi es, en términos generales, el tipo de protección con el que está configurada. Lo puedes comprobar al consultar las propiedades de la conexión desde tu dispositivo (en el menú de Ajustes > WiFi). **Lo ideal es que esté encriptada con cifrado WPA-2** para proteger tus datos y que requiera insertar una contraseña.

Corrobora que es la red adecuada

Para evitar varios de los problemas que te hemos comentado, debes asegurarte de que estás conectándote a la red correcta. Nombres como «WiFi gratis» o «free Internet» suelen ser cebos, así que desconfía de ellos. Lo mejor es siempre que preguntes al responsable del local sobre cuál es la red.

Toma precauciones al registrarte

Si una red inalámbrica no tiene contraseña, seguramente te pida registrarte. Esto sucede mucho en las instalaciones de gran tamaño, como los centros comerciales o las universidades. Ante esta situación, revisa bien qué información te está pidiendo. Nunca aportes datos que no querrías facilitar en otro contexto.

Revisa bien las condiciones

Muy pocas personas leen las condiciones de uso antes de aceptarlas. Sin embargo, esta es una práctica bastante peligrosa, ya que estamos dando autorización para algo que no sabemos. Por tanto, es fundamental que te tomes tu tiempo para examinar con detalle las condiciones. Si no vas a poder asegurarte, nunca las aceptes.

¿Cómo proteger los dispositivos al navegar por redes públicas?

Si has detectado que la red es segura, puedes conectarte. Eso sí, todavía puede haber riesgo, ya que no sabes con qué personas estás compartiendo la conexión. No significa que no tengas que utilizarla, pero **sí que debes tomar varias precauciones**.

Navega por páginas seguras

En realidad, siempre hay que navegar exclusivamente por páginas seguras, incluso si te conectas desde tu red. No obstante, es más peligroso en estas situaciones. Para saber si una web es segura, debes fijarte en dos aspectos:

- **Que el enlace comience por «https»** (no «http») antes de acceder.
- Que aparezca el **icono de un candado** a la izquierda de la dirección (una vez que estás dentro).

No entres a páginas sensibles

Hay páginas que nunca deberías visitar desde una red pública, ya que tus datos de acceso podrían ser robados. Entre ellas, destacan:

- Cuentas bancarias.
- Redes sociales.
- Correo electrónico personal y profesional.
- Página web de la empresa.
- Portal de la aseguradora.

Instala un antivirus

El antivirus debe ser un complemento imprescindible en tu teléfono u ordenador y no solo para estas situaciones. Lo mejor es que tengas un programa o aplicación de protección adecuado y **actualizado a su última versión**. De este modo, te puede advertir sobre una conexión maliciosa o un intento de robo.

Actualiza las aplicaciones sensibles

Cada vez que los equipos de desarrollo de un programa informático o de una aplicación lanzan una actualización, están incrementando también su nivel de seguridad. Muchas personas ciberdelincuentes se aprovechan de las *apps* desfasadas para entrar más fácilmente. Es importante que tengas siempre las redes sociales, aplicaciones bancarias y demás actualizadas a la última versión.

Actualiza tu teléfono

Igual que es importante que tengas las aplicaciones al día, necesitas hacer lo propio con tus dispositivos. Cada vez que tengas un aviso de actualización disponible, **acéptala para que no se acumulen**. De lo contrario, tu teléfono estaría perdiendo garantías de seguridad con el paso del tiempo.

Cuidado con los archivos compartidos

Si recibes un mensaje de una persona desconocida con un archivo adjunto, desconfía. Lo mejor es bloquear al remitente si no sabes quién es y te resulta sospechoso. También es esencial que no abras archivos compartidos a través del correo electrónico o el SMS, ya que puedes ser víctima de *phishing* (robo de datos con fines delictivos).

Entonces, ¿es seguro conectarse a un WiFI público?

Como has podido ver, las redes públicas pueden entrañar algún tipo de riesgo si no se usan de una forma adecuada. Sin embargo, esto no quiere decir que haya que evitarlas siempre. En cualquier caso, **lo más importante es que sepas que navegar por una conexión WiFi pública puede ser seguro**. Para ello, necesitas tomar las precauciones que te hemos comentado.

Un consejo: en caso de que necesites conectarte, intenta hacerlo a través de una red oficial.

En definitiva, **una red WiFi pública puede ser de gran utilidad**, pero hay que utilizarlas con responsabilidad. Para ello, es fundamental que conozcas a dónde te estás conectando y no dar más información de la necesaria.

vuela

1.6

Qué es el *phishing*, cómo te puede atacar y cómo puedes prevenirlo

Hoy en día, cada vez hacemos más uso de los medios *online* para comunicarnos, consumir contenido de entretenimiento o incluso para estudiar y trabajar. A medida que aumentamos el uso de las tecnologías digitales, también debemos incrementar las precauciones que tomamos para que nuestra navegación por Internet sea siempre segura.

Para facilitar esta tarea, en este artículo te explicamos **qué es el *phishing***, uno de los riesgos que más frecuentemente podemos encontrar en la red. Además, también te detallamos cómo puedes identificarlo y te mostramos algunas buenas prácticas de ciberseguridad que seguro que te ayudan a combatirlo fácilmente.

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es el *phishing*?

El *phishing* procede de una variación de la palabra inglesa «*fishing*» (pescar), ya que la o el ciberdelincuente navega por la red con la intención de "pescar" la información privada de las personas internautas. Estas pueden enfrentarse a numerosos problemas al dejar expuesta su información confidencial:

- **Robo de datos personales**: contraseñas en cuentas de todo tipo, dirección, etc.
- **Pérdidas económicas**: en personas que realizan compras por Internet sin tomar medidas de seguridad.
- **Suplantación de cuentas**: sobre todo en redes sociales.

Si lo piensas, igual que ocurre con la pesca, para que esto se produzca la persona objetivo debe "morder el anzuelo". ¿Qué significa esto? Pues que este tipo de ataques consiguen entrar a los ordenadores y teléfonos móviles, sencillamente, porque **se les «abre la puerta» a que se introduzcan en el dispositivo**; por ejemplo, mediante un comportamiento de riesgo o con una seguridad deficiente en el dispositivo.

Por suerte, está en nuestra mano contribuir a que esta amenaza desaparezca. No se trata de abandonar el uso de Internet, sino de todo lo contrario. La clave está en acostumbrarnos a emplear los dispositivos electrónicos y a conectarnos de una forma segura y responsable, tomando las precauciones adecuadas.

¿Cómo puedes sufrir tú un ataque de este tipo?

La mejor manera de evitar ser víctima de *phishing* es saber cómo actúan las personas ciberdelincuentes que realizan este tipo de prácticas y cuidar la protección de nuestros dispositivos. Por ello, te explicaremos cómo pueden entrar a tu teléfono móvil, tu *tablet* o tu ordenador.

Por correo electrónico

Seguramente, habrás visto cómo llegan a tu bandeja de entrada numerosos correos. Muchos de ellos pueden pertenecer a tus entidades contratadas (facturas de luz, agua, etc.). Otros, en cambio, pueden contener promociones en las que te has registrado en las tiendas. Pero ¿y qué pasa con los que tú no has «pedido»?

El mecanismo de entrada más común de este fraude es el correo electrónico. Se trata de un mensaje que aparentemente es normal, pero que contiene un enlace algo sospechoso. Erróneamente, un día decides abrirlo a ver dónde te lleva y acabas en una página que, sin pedirte permiso, te descarga un archivo infectado de virus.

Afortunadamente, no basta con que el correo llegue a tu ordenador. Para infectar tus dispositivos, es necesario que lo abras y que cliques en el enlace que aparece.

Por llamada telefónica

Esta práctica adquiere el nombre de *vishing* cuando se realiza mediante una llamada. En este caso, no es algo tan automático, puesto que hay una persona al otro lado de la línea que está ejecutando ese ataque.

A través de esta técnica, la persona ciberdelincuente te puede hacer creer que es una empresa de, por ejemplo, el gas. Para hacerte una factura supuestamente más competitiva, te pide varios datos. Como las llamadas de venta son muy comunes es habitual facilitar el tipo de datos solicitados. **Lo más común es que solo te pidan tu nombre, tus apellidos y el DNI**. Con esta información, les basta para suplantar tu identidad donde lo deseen.

Para evitar caer en esta práctica basta con evitar facilitar datos personales por teléfono a no ser que hayas contactado tú directamente con la empresa por un canal oficial.

Por mensaje de texto

Los mensajes de texto (SMS) quedaron atrás con la llegada de las aplicaciones gratuitas de mensajería instantánea. No obstante, todavía seguimos comunicándonos por esta vía con centros médicos, tiendas y demás entidades similares. Además, muchas veces recibimos publicidad de compañías telefónicas por este canal.

Esta situación se denomina *smishing*, y funciona de un modo muy parecido a los ataques por correo electrónico. Nuevamente, nos llega un mensaje (esta vez un SMS) con un enlace. Si clicamos en este enlace sospechoso podemos estar poniendo en peligro nuestros dispositivos y la información personal que almacenamos en ellos.

Por una página web falsa

Una persona ciberdelincuente puede suplantar una página que tú consultas diariamente para entrar en tu dispositivo. De esta forma, la simulan en aspecto y contenido para que te cueste notar la diferencia. Por supuesto, siempre es posible detectar algunas diferencias que nos ayuden a identificar la suplantación.

Por redes sociales

Las redes sociales tampoco están exentas de ataques como el *phishing*. Muchas veces, se aprovechan de la confianza de las personas usuarias para entrar en su sistema. Para ello, pueden suplantar el perfil de uno de tus contactos de un modo muy realista, con el mismo nombre, foto de perfil y biografía.

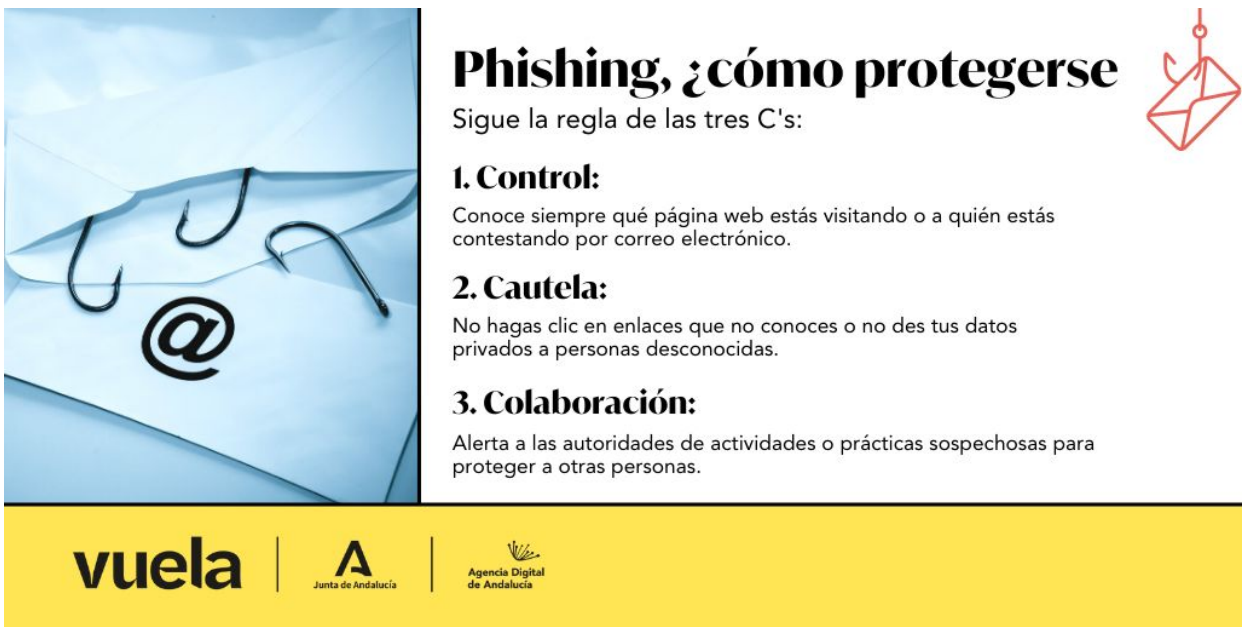
Cuando esta supuesta persona conocida se ha acercado a nosotros mediante una solicitud de contacto, enviará un mensaje con un enlace para que, al clicar en él, accedamos al sitio web malicioso o aceptemos instalar algo en el dispositivo. De las vías que hemos comentado, esta es la que más popularidad está ganando, pero también es la más sencilla de verificar.

¿Cómo prevenir el *phishing*?

Por suerte, puedes emprender buenas prácticas para que las personas ciberdelincuentes no tengan cabida en ninguno de tus dispositivos. Antes de enseñarte cómo hacerlo, vamos a pedirte que pienses en algo que has aprendido en este artículo sin darte cuenta: ¿Cuál es el punto que tienen en común todas las vías de ataque que te hemos comentado? En efecto: **la confianza**.

Cuando vas por la calle o entras en una tienda, nunca confías a la primera de cambio en lo que te comentan. Entonces ¿por qué ibas a hacerlo en Internet? Para evitar riesgos te proponemos que guíes tu actuación en la red por tres criterios:

- Control.
- Cautela.
- Colaboración.



Actuar con **control** implica saber en qué página web estás entrando o a quién le estás contestando ese correo. Por su parte, la **cautela** requiere que no hagas clic en enlaces que no conoces o que no le des tus datos a personas desconocidas. En último lugar, la **colaboración** es básica para que los ciudadanos y ciudadanas podamos alertar a las autoridades ante un intento de ataque.

Para una seguridad mayor, la Guardia Civil recomienda tener un antivirus instalado y actualizado.

Evita sufrir ataques por SMS y correo electrónico

Un correo electrónico o un SMS fraudulento suele presentar varios síntomas que tú puedes aprender a identificar. Desconfía si trata alguno de los siguientes temas:

- Confirmación de una cuenta en una página web a la que no has accedido.
- **Notificaciones de Hacienda** (ni la Agencia Tributaria andaluza ni la española piden datos por estas vías).
- Circulares laborales dirigidas a todos los trabajadores y trabajadoras.

También es importante que elimines los correos o mensajes que tengan un enlace sospechoso o una imagen corporativa de mala calidad. Igualmente, las faltas de ortografía o los mensajes incoherentes son claros indicios de que algo no va bien.

Protégete frente al *vishing* y el fraude por redes sociales

Una llamada fraudulenta puede tener numerosos síntomas diferentes. El más importante lo puedes detectar al saber quién te está llamando (supuestamente). Te dejamos algunos ejemplos:

- Una empresa de suministro: te pide que descargues una aplicación para hacerte un reembolso.
- Un banco: requiere tu número de cuenta o de tarjeta para hacer unas validaciones.
- Una entidad oficial: como puede ser la policía para identificarte por teléfono.

En las redes sociales, puedes **prevenir el *phishing* no aceptando solicitudes de amistad de personas desconocidas**. A su vez, debes desconfiar de mensajes que contengan afirmaciones como las siguientes (que frecuentemente contienen enlaces):

- «¿De verdad eres tú quien sale en este vídeo?»
- «¡Felicidades! Eres el cliente número 1000 y has ganado un sorteo».
- «Para que puedas seguir usando tu cuenta, necesitamos verificar tu identidad».

Detecta páginas web fraudulentas

Sabrás que una web es falsa cuando no tenga estos tres aspectos:

- El icono del candado al lado de la dirección: Significa que la página tiene un certificado de seguridad.
- El término «https» (ojo, no «http») al comienzo del enlace: Implica que tus datos no están expuestos.
- El aviso legal en uno de sus apartados: Todas las webs están obligadas por ley a identificar a su responsable.

Las webs de banca *online* son, por su propia naturaleza, las más seguras. Sin embargo, también pueden haber sido suplantadas, por lo que siempre es recomendable que llames a la entidad si tienes dudas sobre la veracidad.

En definitiva, **el *phishing* es una práctica que podemos y debemos combatir**. Internet es un lugar seguro que puedes utilizar con total tranquilidad siempre y cuando tomes estas sencillas precauciones.

vuela

1.7

Evitar el *spam* y sus riesgos está en tus manos: ¿qué puedes hacer?

El *spam* es un fenómeno muy frecuente en la red y puede llegar a resultar bastante molesto. Además de llenar nuestros dispositivos con comunicaciones no deseadas, esta práctica también puede ser utilizada por ciberdelincuentes para instalar *softwares* maliciosos a través de enlaces o archivos adjuntos. Por ello, en este apartado de nuestra guía te explicamos qué es el *spam*, cómo puedes identificarlo y qué debes hacer para evitar que afecte a tus dispositivos.

Junta de Andalucía

Agencia Digital de Andalucía

¿En qué consiste? ¿Quién lo envía?

También denominado «correo basura», el *spam* consiste en enviar comunicaciones no deseadas y de forma masiva a las personas que forman parte de una lista de correo. Dentro de esta clasificación entran las campañas publicitarias por email que no te interesan, promociones sospechosas que no has solicitado, mensajes en redes sociales e incluso mensajes de texto (SMS) al teléfono móvil. Por esto, se denomina correo basura.

Como ves, el medio utilizado puede variar en cada ocasión, lo importante en todos los casos es que la persona que recibe la información no la ha solicitado ni está interesada en ella.

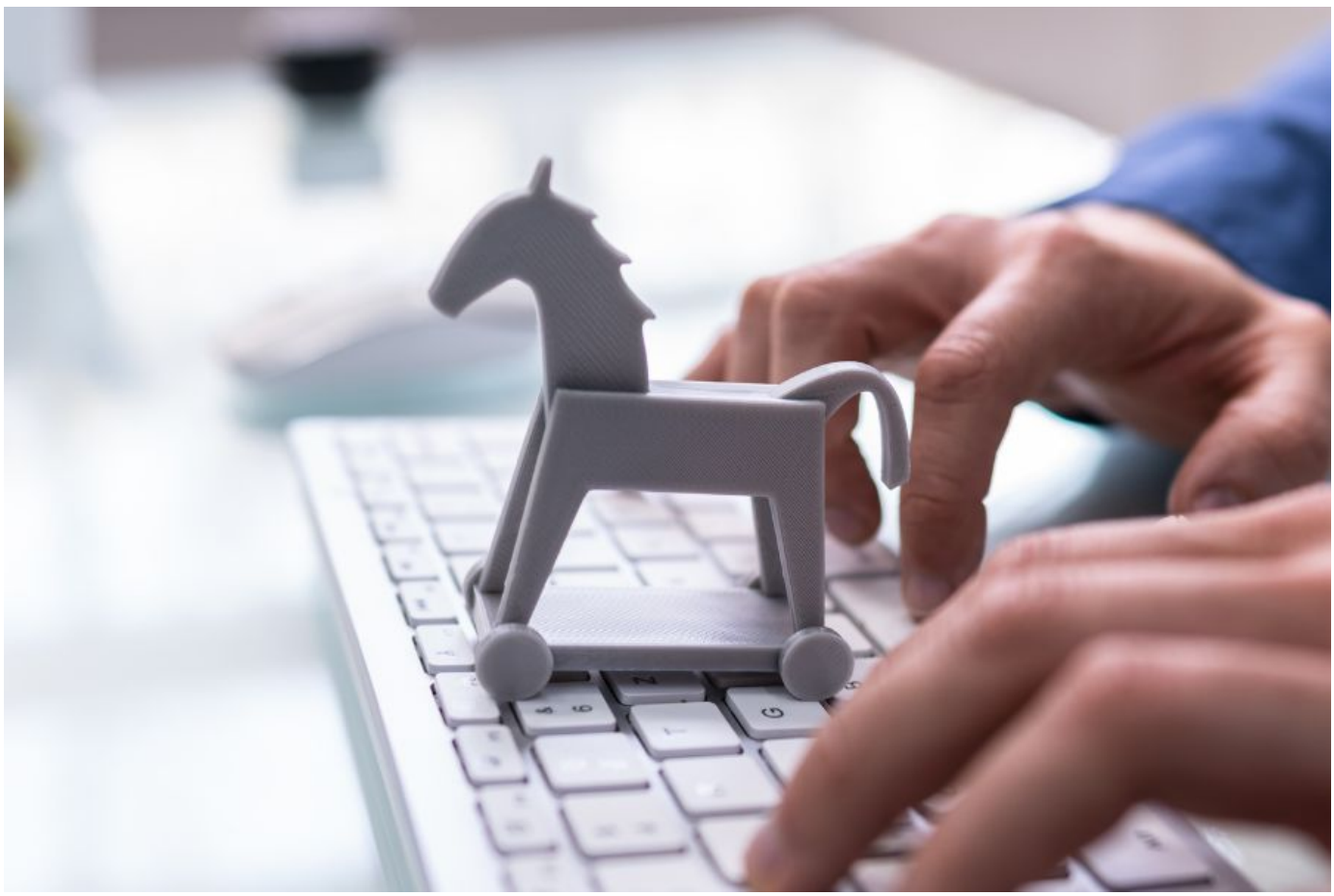
Actualmente, la Ley de Protección de Datos prohíbe expresamente que las empresas puedan enviar correos no autorizados a las personas destinatarias. En consecuencia, **el número de envíos masivos ha disminuido considerablemente**. Entonces ¿a qué se deben los mensajes no deseados que todavía seguimos recibiendo? Principalmente, a tres motivos:

- Muchas veces autorizamos a que nos envíen comunicaciones comerciales sin ser conscientes de ello. Por ejemplo, si no prestamos suficiente atención a las condiciones que aceptamos cuando nos registramos en un sitio web.
- Aunque son pocas, algunas empresas continúan enviando comunicaciones masivas a pesar de las restricciones.
- También hay ciberdelincuentes que recopilan correos electrónicos y números de teléfono de internautas para después realizar comunicaciones masivas o infectar nuestro sistema con algún tipo de *software* malicioso.

Por suerte, la concienciación ha conseguido que el *spam* deje de ser un asunto desconocido. Todos y todas podemos contribuir a hacer de Internet un espacio mucho más seguro y libre de comunicaciones no deseadas. La clave está en no dar continuidad a los mensajes molestos y actuar debidamente cuando recibimos uno (más adelante te daremos varios consejos de buenas prácticas).

¿Puede resultar peligroso?

Además de ser molesto, el correo no deseado puede implicar algunos riesgos a tener en cuenta antes de abrir un mensaje de *spam*. Lo primero que debes saber es que al abrir un email estás exponiendo tu equipo a su contenido, especialmente cuando no sabes quién es su remitente.



El principal riesgo que entraña el correo basura está relacionado con el ***malware*** (virus informático). Este puede estar presente en forma de archivos adjuntos y de diferentes modos:

- Una imagen que introduce un virus al ser procesada por tu ordenador.
- Un vídeo que infecta tus dispositivos mientras lo estás visualizando.
- Una notificación en tu teléfono que te lleva a una página web maliciosa.
- Un enlace que, al clicar, te dirige a un sitio web fraudulento para descargar un virus.

Para que puedas disfrutar de todas las ventajas de interactuar a través de Internet de forma segura hemos clasificado los tipos de *spam* según la vía de entrada, el «gancho» y el propósito. De este modo te será más fácil identificarlo y saber cómo actuar en cada caso.

Según su vía de entrada

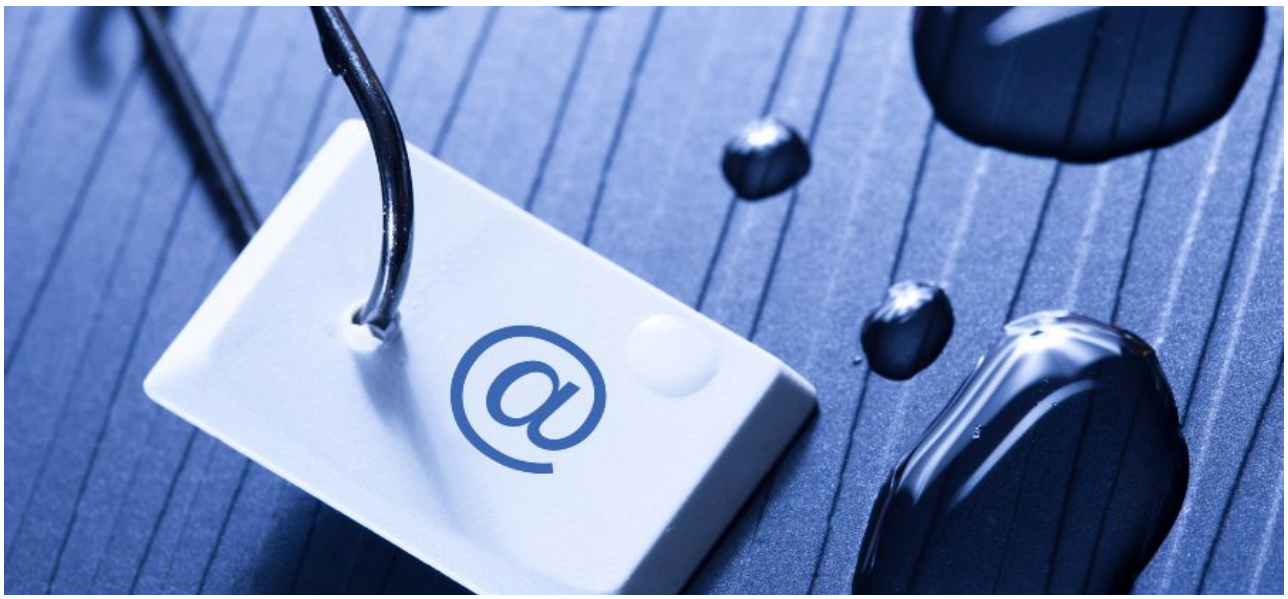
Hasta ahora, hemos hecho referencia al correo electrónico porque es la vía más frecuente. Sin embargo, es esencial que conozcas otras plataformas por las que puedes recibir comunicaciones no deseadas que, a veces, puedan estar infectadas con virus informáticos:

- **Por mensaje de texto (SMS)**. Se trata de mensajes de supuestas entidades, como un banco o una empresa de energía o telecomunicaciones, que te piden que cliques en un enlace.
- **Por mensajería instantánea (chat)**. En las aplicaciones más conocidas también puedes recibir cadenas de mensajes con publicidad no deseada y, en algunos casos, con enlaces fraudulentos.
- **Por *popups* (mensajes en webs)**. Cuando entras en una web maliciosa, es posible que recibas una notificación para permitir el acceso a algún elemento de tu sistema; por ejemplo, a tu carpeta de Imágenes o a ver tus documentos.

Según el «gancho»

Una segunda clasificación tiene en cuenta el «gancho», es decir, el elemento que utilizan para captar tu atención. Es muy importante que conozcas cuáles son los más habituales para que sepas detectar cuándo están tratando de engañarte. De esta forma, identificamos los siguientes:

- **Sorteos y oportunidades**. Mensajes del tipo «¡Felicidades por ser el cliente 1000!» o productos sospechosamente baratos.
- **Estética y salud**. Comparaciones antes / después o supuestos tratamientos milagrosos.
- **Ofertas y descuentos**. Promociones extrañamente atractivas o descuentos muy exagerados.
- **Noticias falsas**. Las denominadas *fake news* que anuncian la muerte de una persona famosa o una catástrofe.



Según su propósito

Por último, también conviene aprender a determinar cuál puede ser el propósito del mensaje que has recibido. Ante la duda de si una comunicación puede ser maliciosa, te recomendamos no abrir su contenido. ¡La prevención es tu mayor aliada! No obstante, aquí te detallamos cuáles son los propósitos más comunes para el *spam*:

- **Hacer publicidad**. Este es el propósito de la mayoría de los mensajes de *spam* que recibimos en nuestro día a día. Para muchos negocios esta práctica es una forma de lograr que siempre tengas presente sus productos o servicios, incluso aunque no te interesen.
- **Infectar tus dispositivos**. A través de los enlaces o de los archivos adjuntos las y los ciberdelincuentes pueden infectar tus dispositivos con virus y otros *software* maliciosos. Recuerda no pulsar ningún enlace ni descargar archivos adjuntos en mensajes de *spam*.
- **Robar tus datos**. Para esto, pueden instalar un programa espía que acceda a la información personal almacenada en tus dispositivos. Como en el caso anterior, evitar las descargas de archivos adjuntos y los clics sospechosos son una gran medida de prevención.

¿Cómo puedes evitar el *spam*?

Si todas las personas usuarias colaboran, lograremos que siga reduciendo su influencia. Lo más importante es que actúes siempre bajo la premisa de «los 3 noes»:

- **No sigas la cadena**. Cuando recibas un mensaje no deseado por cualquier vía, elimínalo y no se lo envíes a nadie más.
- **No caigas en engaños**. Desconfía de las ofertas demasiado atractivas o las páginas con apariencia fraudulenta.
- **No des tus datos**. Antes de facilitar tu correo electrónico a un sitio web asegúrate de leer las condiciones y de que la empresa o marca que gestiona ese sitio web es respetuosa con la Ley de Protección de Datos.

Además de estas tres directrices que deben guiar la conducta de todos y todas, puedes tomar otras precauciones para mantenerlo a raya.

Ten más de una cuenta de correo electrónico

¿Cuántas cuentas de correo tienes? Muchas personas solo gestionan una o, como mucho, dos. Pero te recomendamos que tengas, al menos, tres:

1. **La principal, para tu vida diaria**: trámites oficiales, comunicaciones importantes, etc.
2. **Una de carácter secundario**: para registrarte en foros, empresas y promociones.
3. **Otra para tu vida profesional**: correos de trabajo, ofertas de empleo y demás.

De esta forma, mantendrás la primera y la tercera mejor protegidas, que son las más relevantes. La segunda puede recibir correos basura por parte de negocios en los que te has suscrito, pero no afectarán a tu vida privada ni al trabajo.

Escanear en busca de virus

Todos tus dispositivos electrónicos deben tener un antivirus con licencia y actualizado a la última versión. De lo contrario, tus dispositivos estarán menos protegidos ante este tipo de riesgos y, con ello, tu información personal. De hecho, según el INE, solo el 51,5% de la población española comprueba que un sitio web donde se le pide información personal es seguro y esto puede ocasionar la entrada de *malware*.

La mayoría de antivirus pueden escanear en busca de virus un correo electrónico. Esto te ayudará a saber si puedes abrirlo o no, aunque no te aporta seguridad al 100%. ¿Por qué? Principalmente, porque el virus puede estar en una página web a la que llegas mediante el enlace que aparece en tu mensaje. Nuevamente, recuerda evitar acceder a aquellos enlaces que no sepas seguro a dónde te dirigen.

Crea listas de correo no deseado

En el correo electrónico, tienes una carpeta predeterminada en la que se almacena todo aquello que consideras innecesario (normalmente la identificarás con el nombre de *spam*). Esto no evita que lleguen más mensajes a esta dirección, pero estos se almacenan sin realizar ningún aviso. También puedes bloquearlo para no volver a recibir un correo de ese remitente.

Para ello, tienes que seleccionar el mensaje no deseado en tu bandeja de entrada. Después, te aparecerán una serie de opciones, entre las que destacan «Marcar como no deseado» (o «Marcar como *spam*») y «Bloquear destinatario». Todo depende del gestor de mensajería (Gmail, Hotmail, etc.) que utilices, aunque todos ellos suelen tener **listas de correo no deseado**.

Importante: No intentes cancelar la suscripción

Cuando detectes un correo no deseado, es mejor que **no trates de cancelar tu suscripción**. Muchos ciberdelincuentes o entidades fraudulentas incluyen un enlace que, aparentemente, te permite no volver a recibir sus comunicaciones. Sin embargo, lo único que estás haciendo es confirmarles que tu cuenta está en uso y, por tanto, convertirte en su objetivo. En otros casos, ese enlace puede llevarnos a la descarga de un *malware* (*software* malicioso).

Como te decíamos antes, lo mejor es añadirlos a la carpeta *antispam* o bloquearlos. Además, nunca trates de averiguar el propósito del mensaje si no está totalmente claro. Basta con saber que es un correo que no deseas recibir. Si indagas por tu cuenta, necesitarás abrirlo y, por tanto, será la puerta de entrada a tu dispositivo.

En definitiva, **el *spam* es tan común como evitable**. Lo más importante es que sepas identificarlo y cortes la cadena cuando llegue a tu dispositivo. Así conseguiremos que nuestras bandejas de entrada estén libres de comunicaciones basura.

vuela

1.8

Fraudes por Internet: descubre los más habituales

Seguramente alguna vez hayas escuchado en las noticias hablar de los **fraudes por Internet.** Es cierto que, al igual que nuestra vida cotidiana es cada vez más digital, también cada vez más es en el medio *online* donde se producen las estafas. Sin embargo, lo cierto es que la mayoría de fraudes *online* son fácilmente identificables y basta con tomar unas sencillas precauciones para navegar de forma segura.

A continuación, te daremos **pautas para que puedas seguir disfrutando de todo lo bueno de la tecnología a la vez que te mantienes a salvo de posibles estafas.** Veamos cuáles son las más comunes y cómo podemos evitarlo

Junta de Andalucía

Agencia Digital de Andalucía

Phishing, uno de los fraudes por Internet más habituales

Phishing significa pescar en inglés. Al hacer la traducción ya puedes imaginarte cómo funciona esta estafa. Lo que hace el o la ciberdelincuente es **"lanzar la caña" y esperar a quienes navegan por la red "piquen"**.

A grandes rasgos, su manera de operar es **suplantar la identidad de una entidad en la que confías y hacerse pasar por ella**: Seguridad Social, banco, Netflix, universidad, Hacienda… Normalmente recibes un correo electrónico o un SMS de una empresa o asociación que es de tu confianza. **Suele ser una comunicación que busca crear en ti la necesidad urgente de pinchar en el enlace que va en el mensaje**.

Por ejemplo, puede ser Hacienda diciéndote que tienes una devolución de dinero pendiente de recibir y que necesitan tu número de cuenta bancaria, o la Seguridad Social advirtiéndote de que tienes una deuda pendiente de pago y que debes liquidarla lo antes posible. O puede tratarse sencillamente de Netflix (u otro servicio similar) haciéndote una gran oferta, o hasta tu banco reclamando algún dato personal tuyo que le falta.

Como la persona usuaria confía en el emisor del mensaje y da credibilidad al mismo, **acaba pinchando en el enlace y aportando los datos que se le piden**. Lo que no sabe es que realmente no está accediendo a la web real de la entidad, sino a una copia de la misma. En cuanto introduce datos como el número de su tarjeta de crédito, estos van directamente a manos del delincuente.

¿Qué hace la persona ciberdelincuente con la información? Puede **"secuestrar" tus redes sociales y pedirte un pago para que recuperar el acceso**, usar los datos de tu tarjeta para realizar compras *online*, saquear tus cuentas bancarias, suplantar tu identidad en la red, vender tus datos en el mercado negro, etc.

¿Se puede evitar el *phishing*?

Si alguna vez has ido a pescar es posible que te hayas vuelto a casa sin un solo pez, y eso es lo que deberíamos conseguir cuando una o un ciberdelincuente intenta cometer una estafa de *phishing*: que tire la caña, pero nadie pique.

Para lograrlo, lo mejor que puedes hacer es **no fiarte nunca de las comunicaciones de remitentes desconocidos**. Si no conoces a quien te envía el correo, mejor no te molestes en abrir el mensaje y bórralo directamente. Si la comunicación llega de tu banco, de Hacienda, u otro remitente de confianza, ten siempre presente que **ninguna de estas entidades te va a pedir datos personales a través de un correo electrónico o de un SMS**.

Ante la duda, accede a su web directamente desde tu navegador escribiendo la dirección de la entidad y, si es necesario, contacta con ella para comprobar si la información que has recibido es cierta o es un fraude.

Hasta hace unos años era relativamente fácil identificar los mensajes fraudulentos, ya que solían estar mal redactados y su apariencia ya te hacía sospechar. Sin embargo, las personas delincuentes están cuidando cada vez más este aspecto. Así que no te fíes de una comunicación solo porque esté correctamente escrita o sea visualmente creíble.

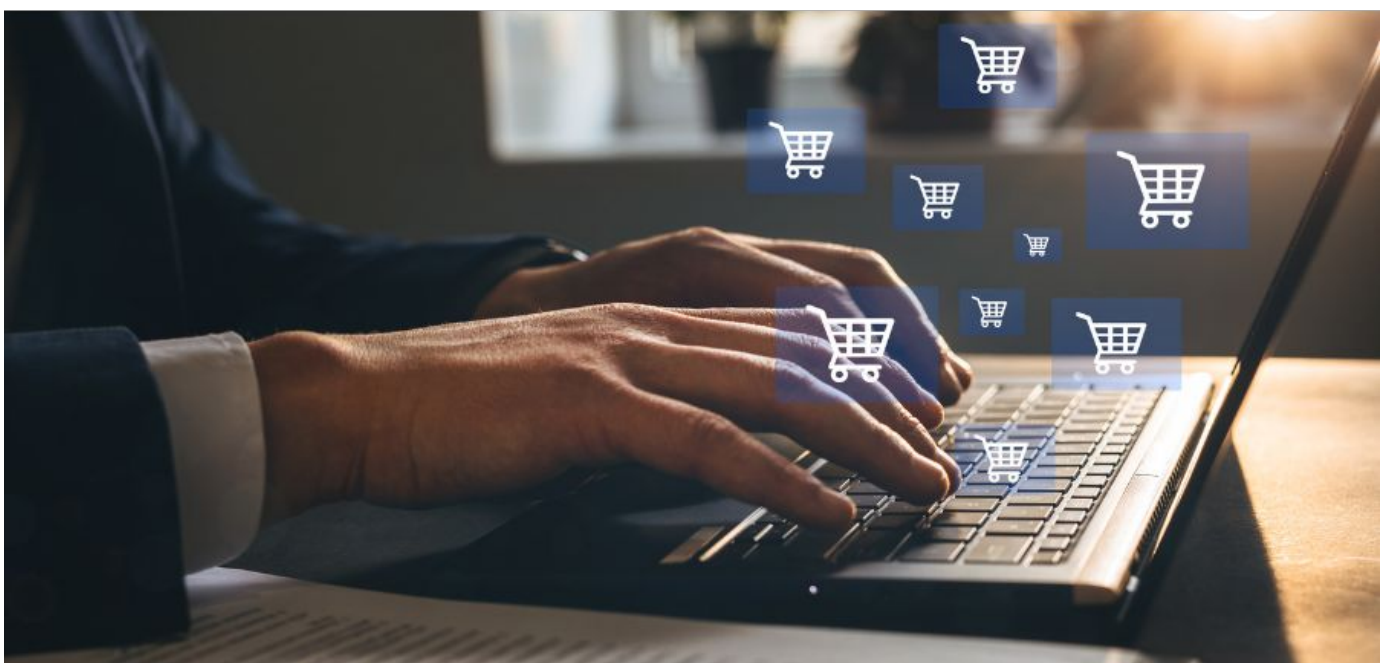
Una última forma de asegurarte de si la comunicación es real es **hacer un corta-pega de todo lo que aparece en la dirección de correo electrónico del remitente a partir de la arroba (@)** y buscarlo en Internet. Si la dirección es legítima, te mandará a la web de la entidad real. Si es ilegítima no te conducirá a ningún lado.

Tiendas *online* fraudulentas

¿Quién no ha hecho una compra *online* alguna vez? El comercio electrónico ha aumentado mucho en la última década y a medida que se ha desarrollado también han crecido los fraudes asociados a esta actividad. Dado que las personas ciberdelincuentes lo que buscan es dinero, no es de extrañar que también creen falsas tiendas *online* para intentar engañar a quienes van a comprar en ellas.

El funcionamiento de este tipo de estafas suele ser similar en todos los casos. Lo que hace el o la delincuente es **crear una web falsa en la que vende un producto con mucha demanda en el mercado a un precio realmente irresistible**. De este modo se despierta la curiosidad de la persona, que pincha en el enlace, y desde allí es dirigida a algo que parece una tienda *online* oficial, aunque realmente no lo es.

En estos casos, **llevarás a cabo el proceso de compra con total normalidad**. Pones el producto en el carrito de la compra, indicas la dirección de entrega y realizas el pago. Incluso es posible que justo después recibas un correo electrónico confirmándote la transacción, que es lo que suelen hacer las tiendas digitales legítimas. No es hasta unos días más tarde cuando te das cuenta del problema: **el paquete nunca llega**, y cuando vas a reclamar a la tienda, descubres que no hay nadie detrás dando soporte.



Esta es una versión de este timo, pero hay varias. Un ejemplo es la empresa vendedora que **entrega un producto cuya calidad tiene poco o nada que ver con lo que se mostraba en la web** (esto pasa mucho con la ropa y el calzado) o la que hace el envío de un paquete lleno de objetos inservibles, como papel o piedras.

No es solo que la persona ciberdelincuente se quede con el dinero de tu compra, es que tiene todos tus datos y puede hacer con ellos lo que desee. Además, **al acceder a su web es posible que se haya instalado *malware* en tu dispositivo**.

Se trata de un programa informático malicioso que puede recopilar tus datos, acceder a tus archivos o supervisar tu actividad *online*, entre otras cosas. **Información que el o la delincuente puede usar para extorsionarte o para vender a terceros**.

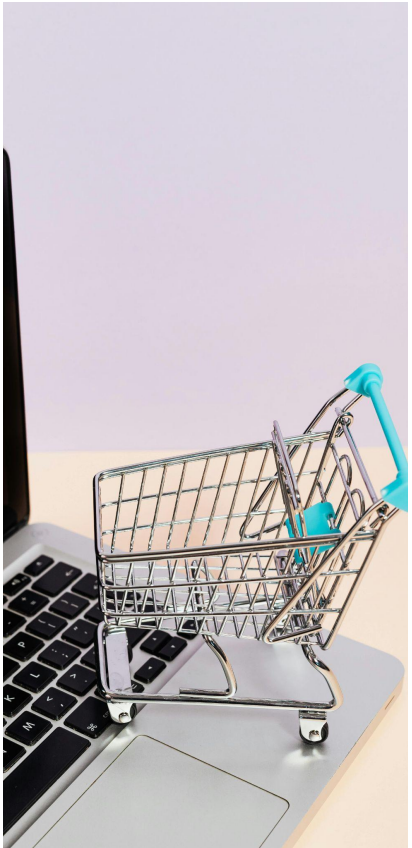
¿Cómo evitar este fraude?

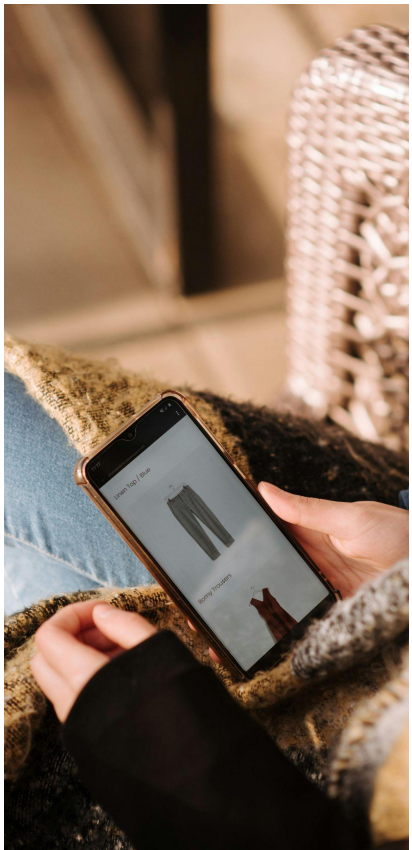
Lo recomendable es que **no accedas nunca a ningún sitio web desde publicidad que veas en canales como las redes sociales**. Si has observado algo que te interesa, mejor que escribas la dirección de la tienda en tu barra de direcciones y accedas directamente desde tu navegador.

Por otro lado, si es un establecimiento que no conoces, no está de más que hagas una labor de investigación previa. **Haz en Google una búsqueda de este estilo: "opiniones sobre (nombre de la tienda)".** Inmediatamente, podrás conocer la experiencia de clientes anteriores, lo que te permitirá saber si es una tienda legítima o una estafa.

Pero no te fíes si no hay opiniones. Puede que el delincuente acabe de crear la web y todavía no haya información suficiente sobre la misma. Recuerda que muchas de las personas que han sido timadas *online* tienen vergüenza de reconocerlo y no advierten a los demás.

Una última cosa a tener en cuenta. **Si la oferta es muy buena para ser verdad, lo más probable es que no sea cierta y se trate de un fraude.**





¿Cómo denunciar estas estafas?

Denunciar delitos informáticos es hoy en día muy sencillo. Si no quieres desplazarte a la comisaría de policía, lo que puedes hacer es denunciar el hecho a través del portal web de la Policía Nacional rellenando un formulario o contactar con las Fuerzas y Cuerpos de Seguridad del Estado a través de redes sociales (puedes hablar con **@policia en Twitter**).

Otra opción es contactar con el Instituto Nacional de Ciberseguridad (INCIBE) y comunicar la incidencia por correo electrónico. Y no estaría de más **avisar a la entidad cuyo nombre están usando los delincuentes para engañar a las personas** (si es un caso de *phishing*).

Recuérdalo, para evitar los fraudes por Internet lo mejor que podemos hacer es **prestar mucha atención a los sitios por los que navegamos**, asegurarnos bien antes de comprar nada o dar nuestra información y, si vemos algo extraño, denunciarlo. **Con cada denuncia interpuesta nos protegemos todos y todas**.

vuela

Protégete ante los riesgos

Para evitar la mayoría de las amenazas de Internet basta con tomar algunas precauciones. En este apartado te enseñamos cómo proteger nuestros datos personales y cuidar la privacidad frente a posibles atacantes.

2

Junta de Andalucía

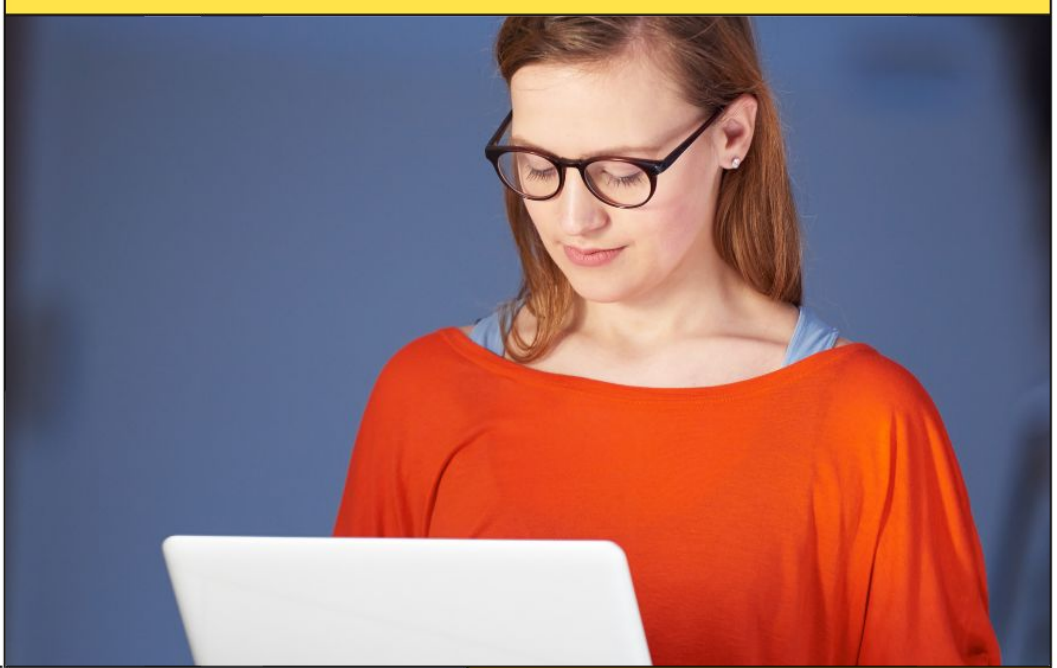
Agencia Digital de Andalucía

vuela

2.1

Contraseñas: crea y almacena tus passwords de forma segura

Las **contraseñas** o ***passwords*** son tu **primera línea de defensa ante un ataque cibernético.** Si las eliges correctamente, las posibilidades de sufrir un asalto a tu privacidad se reducen considerablemente. Estas herramientas de seguridad son necesarias para identificarte en cualquier punto de la red, comenzando desde el propio *email* o correo electrónico. En las diferentes redes sociales también tendrás que seleccionar una, así como en distintas páginas webs. Hay incluso páginas que te señalan si la contraseña o el código de verificación que estás creando es inseguro y te piden modificarlos, añadiendo ciertos caracteres para reforzarlo.



Junta de Andalucía

Agencia Digital de Andalucía

Como ves, compatibilizar Internet y seguridad puede ser una tarea muy sencilla y que cualquier persona puede llevar a cabo. Para ello no necesitas contar con grandes conocimientos informáticos, únicamente **mantener un comportamiento responsable cuando navegas por la red** y prestar atención a las herramientas de seguridad a tu disposición, como las contraseñas.

Pautas para establecer contraseñas seguras

A la hora de seleccionar *passwords*, hemos de **obviar aquellas que puedan ser fáciles de adivinar**. Es decir, no pongas datos que cualquier persona de tu día a día podría conocer fácilmente, como el nombre de tu mascota, la fecha de tu cumpleaños o de alguna persona de tu familia. **Lo ideal es que tu contraseña solo la conozcas tú**, así como en qué te has basado para elegirla.

Dependiendo de para qué estés usando este código de autentificación, las propias páginas o aplicaciones te pedirán cierto tipo de medidas extraordinarias para lograr una **contraseña fuerte** o robusta. La mayoría de las veces, esto implica que debe tener al menos **8 caracteres** y estar compuesta por: **mayúsculas**, **minúsculas**, **números** y algún **carácter especial**, como & o *.

Crear una contraseña con estas características siempre es buena idea, aunque la propia web no te lo solicite. Puedes emplear ciertos **patrones** a la hora de crear una, como el siguiente:

- Elige un **símbolo especial**, el que prefieras.
- A continuación, selecciona una **palabra** o unas **siglas** que puedas recordar fácilmente, e introduce al menos una de las letras en mayúscula.
- Por último, introduce un **número**.

Si haces esto y diseñas un patrón que puedas recordar fácilmente, nunca tendrás problema a la hora de recordarla. Lo ideal sería que la **cambies cada cierto tiempo**, puesto que haciendo esto aumentas la seguridad, y que evites compartirla a no ser que sea estrictamente necesario. En ese caso, no compartas nunca los datos mediante conversaciones de WhatsApp o mediante correos electrónicos.

Otro consejo a la hora de conseguir *passwords* seguros es **no utilizar la misma clave para todas las cuentas**. Puede parecer lo más sencillo y lo más lógico, pero si en algún momento dado se revela este dato, otras personas podrían tener acceso a todas tus cuentas. Es por eso que es buena idea que optes por **contraseñas distintas** para cada red social o para cada cuenta que abras en Internet.

Algunos buenos **ejemplos de contraseñas seguras** serían: *Azul3, &pcJuan893, 90mArron#. Recuerda que debes cambiar tanto la palabra como los números y símbolos de vez en cuando, y que lo mejor es que selecciones algo de lo que puedas acordarte sin complicaciones.

Un generador de contraseñas especiales

Si te parece complejo el proceso de creación de tu código de verificación o contraseña, siempre podrás optar por usar **un generador de contraseñas con caracteres especiales**.

Básicamente, consiste en un programa que te permite crear *passwords* con un alto nivel de seguridad. Genera una contraseña totalmente aleatoria, combinando letras en mayúscula y en minúscula con números y otros caracteres especiales.

Emplear este tipo de herramientas es muy **sencillo**, puesto que solo tienes que acceder a la página web del generador y pulsar el botón de '**Generar contraseña**'. A partir de ahí, ya tendrás una **combinación de caracteres que sea robusta** y que podrás utilizar en cualquier web. Además, podrás confiar plenamente en que el resultado que obtengas sea seguro, porque nadie podrá adivinarla.

Si confeccionas tu propio *password* y dudas de su fortaleza, o piensas que puede ser fácilmente adivinado por alguien que te conozca, lo mejor es que optes por una herramienta de este tipo. Algunas de las webs que puedes utilizar son clavesegura.org o generarclave.es.

¿Cómo guardar las contraseñas de forma segura?

Seguramente, llegados a este punto, te estés preguntando **cómo vas a poder recordar todas las contraseñas** si todas tienen esas complejas combinaciones de números y letras, además de ser diferentes. Te vamos a dar varias **claves** para que jamás las olvides, pero también para que estas continúen siendo seguras:

- **Pásate al papel y al bolígrafo** a la hora de almacenar los *passwords*. Parece una obviedad, o un paso atrás, pero lo cierto es que es un **método seguro** siempre y cuando sigas las siguientes recomendaciones. Debes apuntarlas en una libreta o en un folio, y guardarlo a buen recaudo. No las apuntes en la agenda o en cualquier otro cuaderno que lleves siempre encima. Guárdalas siempre en tu casa, para que nadie tenga acceso a ellas. De esta manera, nadie podrá acceder a ellas mediante un ataque cibernético. Por supuesto, para garantizar que este método es seguro, no almacenes el listado de tus contraseñas en un documento en tu ordenador.
- Si prefieres optar por un **método más digital**, descárgate un **gestor de contraseñas** tanto para tu ordenador como para tu móvil o *tablet* (1Password, Dashlane, Bitwarden y Roboform son algunas opciones). Este tipo de programas te permite **autocompletar** los *passwords* que ya hayas guardado previamente, y así no tendrás que recordarlas siempre. Además, si la cambias, siempre podrás actualizarla. Eso sí, no olvides nunca la contraseña de este gestor, puesto que será la que te permitirá realizar el resto de funciones.
- El método más cómodo es **aprovechar el propio gestor de contraseñas que suelen llevar consigo tanto los ordenadores** como demás dispositivos a día de hoy. Gracias a la opción de 'Recordar contraseña', tu ordenador podrá completarla automáticamente cuando te la vuelvan a solicitar. Es mucho más cómodo y no necesitarás gestores externos. Los sistemas operativos actuales disponen de gestores de códigos de acceso incorporados. Por ejemplo, el de *Apple* se llama *Keychain* y te pide siempre una comprobación de que eres tú para rellenar cualquier dato automáticamente.

La importancia de la seguridad en Internet: consejos que te pueden ayudar

La **ciberseguridad** o seguridad de la información abarca todo aquello que hacemos para que Internet sea un espacio más seguro. Como ya te hemos adelantado, esto implica mantener ciertas **precauciones cuando navegamos por la red**, conocer los riesgos para saber cómo evitarlos y, por supuesto, utilizar algunas herramientas de seguridad como contraseñas o antivirus.

Además, hay algunos **consejos** que es interesante anotar:

- **No uses**, en la medida de lo posible, **conexiones a Internet** que **desconozcas**. Si ves una red abierta en la calle, lo mejor es que omitas emplearla, porque no sabes exactamente de quién es esa red o cuál es el uso real que hace de ella. Si puedes, accede a redes de empresas u organismos públicos que las ofrezcan, puesto que suelen mirar por la privacidad de sus personas usuarias.
- Si estás en un ordenador que no es tuyo, ya sea porque es público o porque es de otra persona, **no le des a 'recordar contraseña'**. De hacerlo, le estarías dando acceso a tu cuenta a todo aquel que tenga acceso a ese dispositivo después de ti. Si lo has hecho sin darte cuenta, cámbiala de forma inmediata y utiliza la opción de cerrar sesión en todos los dispositivos.
- Es más, puedes optar por navegar con el **modo incógnito** si quieres que tus datos no sean almacenados de ningún modo. Normalmente lo encontrarás dentro de las opciones del navegador o junto a la barra de direcciones.

vuela

2.2

Configura tu *router* correctamente para una mayor seguridad digital

Si quieres disfrutar de una **conexión WiFi, ADSL o de fibra óptica** debes disponer de un ***router***. Este aparato se encarga de distribuir la conexión a Internet hacia los distintos dispositivos vinculados a una misma red local: teléfonos, *tablets* u ordenadores. Por tanto, el *router* actúa de intermediario entre el conjunto de equipos e Internet, como un puente entre nuestros dispositivos y la red de redes.

Como ves, resulta un aparato de gran utilidad, por eso aquí aprenderás cómo **mantenerlo configurado correctamente para mejorar tu seguridad digital.**

Junta de Andalucía

Agencia Digital de Andalucía

En la mayor parte de los casos, la instalación del *router* se realiza por parte de la operadora de servicios de Internet y será esta empresa la encargada de comenzar a trabajar la seguridad de este aparato. Aun así, es conveniente que si vas a hacer uso del *router* lleves a cabo algunas pequeñas acciones para mejorar su conectividad, control y seguridad.

Para que entiendas la importancia de cuidar regularmente la seguridad del *router*, piensa que un aparato mal configurado puede dejar tu red digital abierta a todo tipo de ataques cibernéticos y comprometer tus datos privados.

Cómo puedes mejorar la seguridad de tu *router*

A continuación te explicamos algunas pautas que puedes realizar en apenas unos minutos para aumentar la seguridad de tu *router* frente a las posibles ciberamenazas y ahorrarte problemas en el futuro. Si lo haces, aumentarás las defensas de todos tus dispositivos.

Es fundamental la **seguridad en redes WiFi para proteger la red de tu casa**. Seguir estos pasos te ayudará a blindarla.

Actualiza el *firmware*

El *firmware* es una de las partes más importantes del *router*, ya que es el encargado de gestionar todas las conexiones de red de manera óptima y también es una barrera de protección frente a los ataques informáticos.

Como ocurre con la mayoría de herramientas digitales, es recomendable que el *firmware* se encuentre actualizado a su última versión, pues los fabricantes corrigen en cada actualización los errores de seguridad que se han ido detectando.

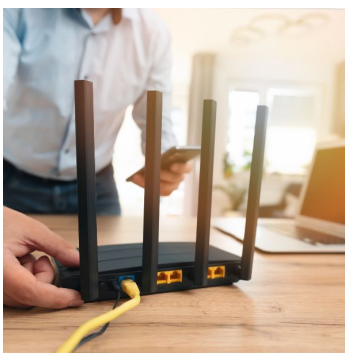
Para asegurar que esta herramienta se encuentra actualizada tendrás que acceder a la web oficial de tu ***router***, acudir a la sección de Soporte o Ayuda y observar cuál es la última versión que se ha publicado del *firmware*. Si no es la que tienes, puedes descargarla e instalarla en tu ordenador desde esa misma web.

Utiliza una contraseña WiFi segura

Para mejorar la seguridad de este dispositivo resulta fundamental que **cambies la contraseña que viene por defecto** para acceder a la red inalámbrica. Es decir, la contraseña que encontrarás en la caja del *router* o en una etiqueta pegada en el lateral del aparato.

Cuando modifiques la **contraseña de administrador** no uses información sencilla que cualquier persona pueda conocer con facilidad, como tu fecha de nacimiento, el nombre de algún familiar, el de tu mascota, etc. Combina minúsculas, mayúsculas, números y algún símbolo. Además, cuanto más larga sea, más dificultad tendrán los ciberdelincuentes para adivinarla.

Hoy en día, **todos los *router* soportan cifrados fuertes como WPA-2** que pueden contar con hasta 63 caracteres. Este sistema es el más recomendable y su activación es muy sencilla. Para ello, entra en tu ***router*** (más adelante explicamos cómo hacerlo), ve a *Wireless Settings*, *Security* y en *Authentication Type*, mueve la pestaña a **WPA-2**.



Desactiva el acceso remoto

El acceso remoto es una opción que permite acceder a la red desde cualquier punto que disponga de acceso a Internet, es decir, permite a la persona usuaria acceder a su red desde otra red distinta. Esta puede ser otra **manera mediante la que personas desconocidas puedan acceder a tu red doméstica**.

Si te aseguras de que esta función está desactivada habrás ganado más seguridad en tu red. Para hacer esto deberás conocer la puerta de entrada a tu dispositivo, algo de lo que hablaremos más adelante.

Riesgos que puedes correr si no tienes tu *router* correctamente configurado

Cuando este dispositivo no cuenta con la configuración adecuada ni con las suficientes medidas de seguridad, está expuesto a una serie de riesgos:

- **Pueden robar tu información personal**: Una persona que tenga suficientes conocimientos podrá acceder a cualquier tipo de información privada que tengas en tu ordenador o móvil. Además, también podrá disponer de los datos que estés enviando y recibiendo a través de Internet.
- **Tu ancho de banda se verá disminuido**: Las conexiones tienen una capacidad determinada que se denomina ancho de banda, de modo que si hay varios equipos conectados a la misma red la velocidad de Internet será más lenta. En función del número de personas que puedan tener acceso a tu red, esta puede llegar a dejar de funcionar o se te hará muy complicado utilizarla: los vídeos se pararán constantemente, las páginas web tardarán mucho tiempo en abrirse, etc.

- **Cualquier acción ilegal estará asociada a ti**: Cuando contratas una conexión, tu proveedor vincula una dirección IP con el nombre del titular, es decir, tú. Cualquier acción ilegal que pueda realizar una persona que acceda a ella estará asociada a tu nombre. Aunque posteriormente puedas demostrar que no fuiste culpable, lo ideal es que te asegures antes de que nadie haga cosas en tu nombre.
- **Tus dispositivos pueden verse infectados**: Cualquier persona cuyo objetivo sea instalar algún tipo de virus en tu dispositivo lo podrá hacer si consigue tener acceso a tu red. Si esto ocurre puede repercutir en tu seguridad y en la de tu ordenador o teléfono móvil, y poner en riesgo la información que almacenes en estos dispositivos.

¿Cómo puedes saber si tu *router* ha sido atacado?

Es posible que te surjan dudas de si en algún momento tu *router* ha podido ser atacado o si incluso hay alguien accediendo a él en ese mismo momento. En este sentido, hay una serie de aspectos que te aportarán información fundamental para saber si esto ha sucedido:

- **Detectar problemas en la velocidad o cortes**: es una de las señales más claras de que algo está ocurriendo. Si te conectas a la red y notas que va excesivamente lenta, que se producen cortes de conexión, que no funciona, etc., la causa podría ser que alguien la está utilizando a la vez que tú.
- **Un parpadeo excesivo en las luces del *router***: este no es un indicativo claro e indiscutible de que algún intruso está usando tu red, pero en algunas ocasiones puede servir de pista. Las luces parpadean en función de la actividad. Si en un determinado momento no estás utilizando Internet y observas que la luz parpadea constantemente, es posible que haya alguien usando tu conexión.
- **Cambios en la configuración**: presta atención si observas cambios en la propia configuración del dispositivo que tú no has realizado. Estos cambios pueden ser **modificaciones en su potencia, cambios de contraseña**, encontrar los **puertos abiertos** cuando tú los tenías cerrados, etc. Los puertos son los canales que utiliza el *router* para enviar datos desde tu red local a la externa. Aunque es más seguro mantenerlos cerrados, a veces puedes abrirlos manualmente para que mejore la conexión. Esto se hace entrando en la configuración del dispositivo.
- **Entrar en el propio *router* y ver los dispositivos conectados**: es la manera más precisa de saber si hay algún intruso en tu red. Solo es necesario acceder al dispositivo y ver los equipos que están conectados en ese momento o lo han estado con anterioridad.

Cómo entrar al *router* para cambiar la configuración y mejorar la seguridad

Cada ***router*** cuenta con una IP que funciona como puerta de entrada predeterminada. Se trata de un código de cuatro combinaciones numéricas separadas por puntos. Las más habituales son 192.168.0.1 y 192.168.1.1.

Escribe una u otra en la barra del navegador para saber cuál es la de tu dispositivo. Luego entra en Configuración avanzada, Información del dispositivo y DHCP. De esta manera, podrás realizar los cambios que desees y comprobar si alguien está conectado a tu red o lo ha estado en algún momento.

¿Qué son los *routers* profesionales?

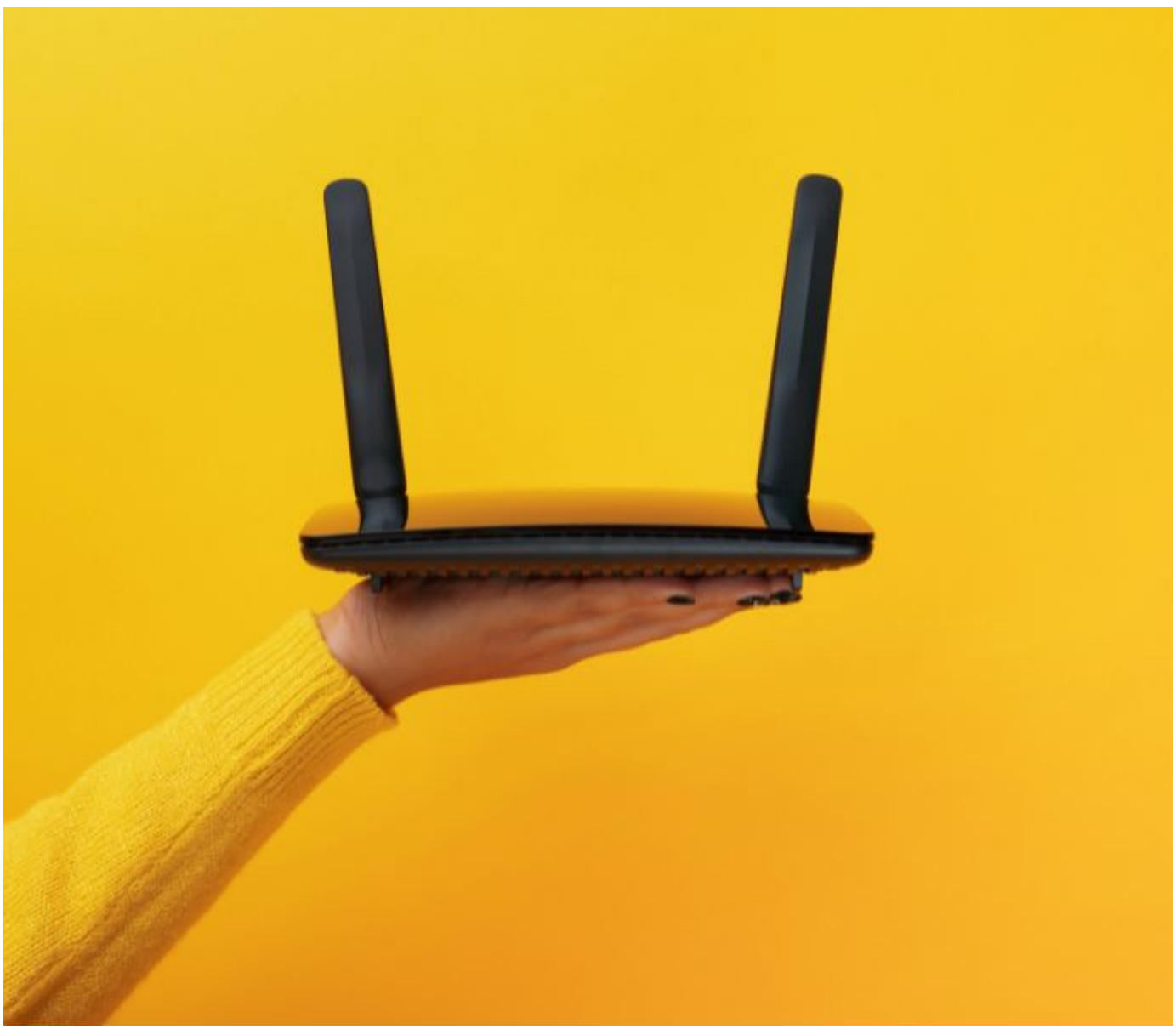
La mayoría de las personas utilizan el *router* **que les ofrece su** proveedor. Sin embargo, existen otros más profesionales que, además de mejorar con creces tu conexión, consiguen **proporcionar un extra de seguridad.** Este tipo de aparatos también facilitan un alcance mayor en tu red WiFi.

Pero además de **mayor alcance y mayor velocidad en la conexión**, lo más importante que aportan estos dispositivos profesionales es su **seguridad y personalización**. Con estos dispositivos puedes cambiar el nombre de la red y las claves. Además, cuentan con actualizaciones que **cubren posibles brechas de seguridad que se hayan podido abrir, cortafuegos y control parental**.

Aunque los que te ofrece la operadora se pueden personalizar en ciertos aspectos, un *router* profesional te ofrece innumerables opciones de configuración para que realices las modificaciones que consideres necesarias por tu propia seguridad. Algunos de ellos puedes llegar a gestionarlos desde una aplicación de tu móvil, de un modo rápido y sencillo.

En definitiva, aunque existen determinados riesgos a la hora de navegar por Internet, si tomas precauciones tan sencillas como las que te hemos explicado será mucho más difícil que algún intruso pueda acceder a tus dispositivos.

Es recomendable que sigas estos consejos, ya que la seguridad de tu red será completa y solo podrán acceder a ella las personas que tú quieras que lo hagan. Al configurar tu *router* de la manera correcta, tu seguridad digital será más sólida y podrás disfrutar de todas las ventajas que tiene disponer de una buena conexión a Internet.



vuela

2.3

Navegador actualizado: su importancia y cómo puedes llevarlo a cabo

El navegador es el programa que utilizamos para acceder a Internet desde nuestro teléfono móvil, *tablet* u ordenador. Entre los más conocidos podemos encontrar algunos como Mozilla Firefox, Google Chrome, Opera, Safari y Microsoft Edge. Independientemente del navegador que utilicemos, todos tienen una característica común: hay que mantenerlos actualizados para que sean seguros.

Junta de Andalucía

Agencia Digital de Andalucía

Si lo piensas, el navegador es tu puerta de entrada a la red y, como ocurre con todas las puertas, es necesario que sea segura para que cumpla con su función de manera adecuada. Con este propósito, los navegadores diseñan periódicamente actualizaciones con el objetivo de proteger frente a las nuevas amenazas que surgen en Internet y corregir errores y vulnerabilidades. De esta manera, al utilizar la última versión de tu navegador siempre contarás con el máximo nivel de protección.

¿Por qué es tan importante mantener tu navegador actualizado?

Según un estudio de la empresa de antivirus y herramientas de seguridad Kaspersky, dos de cada diez internautas no mantienen actualizado su navegador habitual. Como ya hemos explicado, esto supone un riesgo tanto para el equipo desde el que nos conectamos a Internet como para la información que guardamos en él.

Para aportar una protección extra a tus dispositivos, recuerda actualizar tu navegador desde el mismo momento de la compra de tu ordenador, teléfono móvil o *tablet* y convierte en un hábito la revisión periódica del navegador para garantizar que cuentas siempre con la última versión disponible.

Además, recuerda que la seguridad de tus dispositivos no depende del navegador utilices, sino del mantenimiento que hagas del mismo. Existe una falsa creencia en Internet de que hay navegadores seguros y navegadores inseguros. Lo cierto es que el nivel de seguridad de un navegador dependerá de la frecuencia con la que lancen actualizaciones. Cuanto mayor sea esta frecuencia, mayor protección está ofreciendo frente a las amenazas de nueva aparición.

No obstante, la mayor parte de los **ataques informáticos** se llevan a cabo desde páginas electrónicas que explotan las vulnerabilidades existentes tanto en extensiones como navegadores que se encuentran sin actualizar. Dicho de otro modo, los y las ciberdelincuentes no buscan un tipo de navegador en concreto, sino navegadores sin actualizar.

¿Cómo saber si un navegador está actualizado?

A continuación, vamos a detallar algunas **indicaciones** que te permitirán comprobar fácilmente si los navegadores que utilices para conectarte a Internet desde tus dispositivos han recibido ya alguna actualización o si, por el contrario, es necesario que la realices cuanto antes. Para poder acceder a esta información tendrás que seguir la barra de menú.

- En el caso de **Opera**, existe una opción en el menú Ayuda denominada 'Comprobar actualizaciones'. Aquí conocerás cuál es la versión actual.
- **Mozilla Firefox** es un navegador cada vez más utilizado. Su menú de Ayuda cuenta con una pestaña encargada de revisar si hay versiones más modernas: 'Buscar actualizaciones'.
- El más popular y el que es posible que estés utilizando ahora mismo es **Google Chrome**. Para averiguar qué versión emplea y sus posibles actualizaciones debemos acceder a 'Ayuda' y luego pulsar en 'Información de Google Chrome'.
- Si utilizas **Safari** como tu navegador predeterminado puedes identificar la versión que estás utilizando desde el apartado 'Sobre Safari'. Para acceder a este apartado solo tienes que abrir una pestaña en tu navegador y pulsar 'Safari'.

- En el caso de **Microsoft Edge**, al abrir una nueva ventana de navegación selecciona 'Configuración y más' en la esquina superior derecha y, después, selecciona 'Configuración'. Una vez allí, encontrarás toda la información sobre las posibles actualizaciones pendientes en 'Acerca de esta versión'.
- Para comprobar el estado de las actualizaciones del navegador de tu teléfono móvil debes acudir a tu biblioteca de aplicaciones y seleccionar 'Gestionar Apps' en el caso de Android o pulsar en el icono de tu perfil para dispositivos iOS.

Activa las actualizaciones automáticas

Las versiones actuales que emplean los principales navegadores web en Internet, como es el caso de Firefox, Google Chrome o Internet Explorer, ya cuentan con mecanismos que ofrecen una actualización automática a la versión más reciente. En este sentido, el sistema tiene una aplicación que gestiona, descarga e instala, sin la intermediación de las personas usuarias, las **últimas versiones** de sus herramientas en segundo plano.

No obstante, es conveniente asegurarse de que las actualizaciones han sido realizadas exitosamente. Para ello, el primer paso es reiniciar el navegador. Cada uno funciona de forma distinta, por ejemplo, **Google Chrome** se encarga de este procedimiento, sin embargo, no comunica a la persona usuaria que es necesario ejecutar la aplicación para completar el trámite. **Firefox**, por su parte, sí que comunica esta información mediante una notificación en el momento en el que han transcurrido más de 24 horas sin que se haya reiniciado.

Comprueba también la actualización de sus extensiones

Lo primero que tenemos que tener claro antes de comprobar nada es lo siguiente: ¿qué es una **extensión**? Las extensiones son elementos propios del navegador, también denominadas complementos. Se trata de programas de pequeño tamaño que se instalan para mejorar el funcionamiento de los navegadores o añadirles nuevas funcionalidades.

Aparte de revisar si los navegadores vinculados a los equipos que utilizas han actualizado su *software*, también es oportuno repetir este proceso con los **complementos instalados en el navegador**. Lo ideal es utilizar las últimas versiones de estos complementos o *plugins*. Algunas de estas extensiones, como Adobe Flash, Java o Microsoft Silverlight, son las que permiten disfrutar del contenido multimedia. La desactualización de estas herramientas puede ocasionar problemas de seguridad en los equipos informáticos.

Otras ventajas de utilizar la última versión de tu navegador

Una rapidez mayor

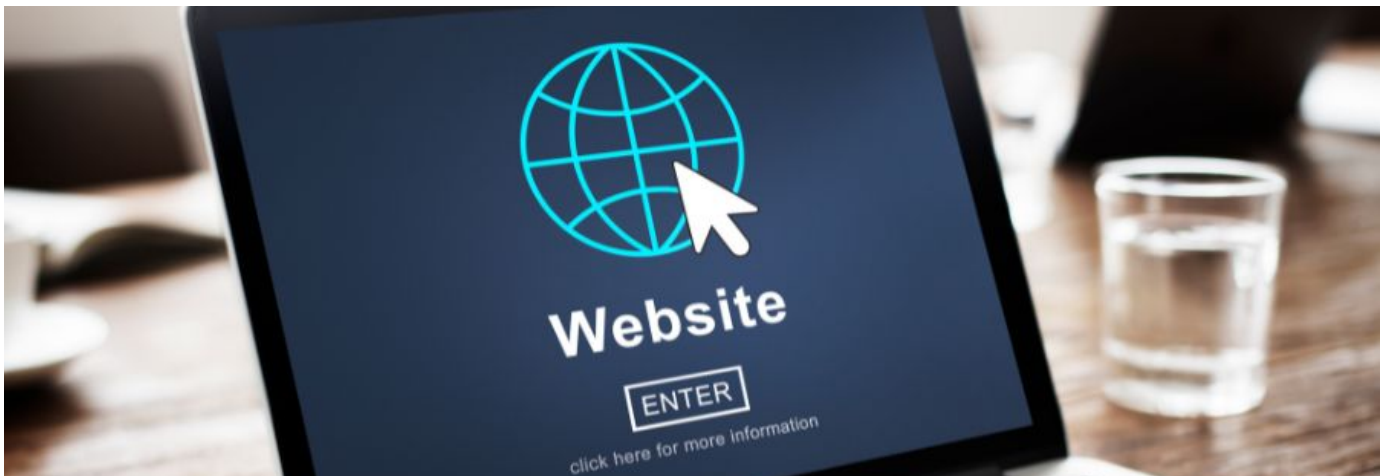
No solo se trata de seguridad, puesto que la **velocidad de carga** de las páginas web es otra de las ventajas que más valoran las personas que acceden frecuentemente a Internet. Los navegadores actualizados incorporan los **últimos motores de búsqueda**. Estos motores consiguen cargar las páginas web mucho más rápido, ya que están optimizados y han dejado atrás los errores de las versiones obsoletas.

Por otro lado, los más modernos son capaces de navegar por Internet sin sufrir ningún tipo de problema relacionado con **incompatibilidades o problemas de carga en los contenidos**. Se debe a que sus versiones actuales incorporan novedades tecnológicas que los convierten en auténticos todoterrenos del ciberespacio. Lo notarás especialmente cuando accedas a **redes sociales** como Instagram, Twitter o Facebook o a servicios virtuales de Google como **Gmail**.

Además, muchos de los lugares web mencionados son a día de hoy incompatibles con las versiones obsoletas de los navegadores web, como es el caso de Internet Explorer 6. Por tanto, aparte de contar con una velocidad de carga mayor, las actualizaciones también te permitirán acceder a tus redes sociales o servicios virtuales favoritos sin problema.

Obtener mayor funcionalidad con menor consumo de recursos

Las versiones obsoletas, al no estar tan depuradas y optimizadas, utilizan una gran cantidad de recursos a la hora de navegar en Internet. Esta es una de las razones más frecuentes para explicar por qué una página tarda tanto en cargar su contenido. En este sentido, un ordenador que mantenga sus navegadores actualizados será **más eficiente**.



Una asistencia técnica también mejorada

Entre los beneficios de actualizar con frecuencia nuestro navegador también se encuentra la ventaja de que las compañías que diseñan estas herramientas ofrecerán para sus últimas versiones un servicio de asistencia técnica y una atención al cliente mejores y **acordes a nuestras necesidades actuales**. Cualquier posible fallo técnico, de *software*, relacionado con datos personales o contraseñas se lo podremos comunicar a la compañía desarrolladora y, gracias a las ventajas de las nuevas versiones, nos atenderán de forma veloz e intuitiva. Las medidas de asistencia antiguas se quedan obsoletas debido a que el personal de la compañía ya no garantiza ni su seguridad ni la resolución de problemas.

Privacidad en Internet

Mantener el anonimato y la privacidad de nuestra información en el mundo cibernético es un derecho fundamental. No obstante, en ocasiones los navegadores no actualizados suponen un riesgo y pueden ser una ventana para aquellos ataques informáticos que tengan como fin sonsacar nuestros **datos personales**. Por este motivo, es de gran importancia cuando navegamos actualizar nuestro *software* de navegación, ya sea Firefox, Opera, Google Chrome o cualquier otro. Como has podido comprobar, mantener tu **navegador** en óptimas condiciones y actualizado supone una gran ventaja a la hora de pasar tu tiempo en la web. Te garantiza, sobre todo, seguridad, una mayor velocidad de carga y la posibilidad de contactar con el desarrollador.

vuela

2.4

Descargas: las claves que debes conocer para protegerte eficazmente

Las descargas de archivos son una parte importante del día a día en Internet, ya que nos ayudan a compartir contenido entre plataformas e internautas. Por desgracia, hay ciberdelincuentes que utilizan las descargas para colarse en nuestros dispositivos y llevar a cabo acciones perjudiciales para nuestros intereses.

Afortunadamente, vigilar los archivos que descargamos para garantizar la seguridad en la red es una tarea sencilla que puedes poner en práctica hoy mismo. De hecho, **la mejor herramienta a tu alcance es la precaución.** Por ejemplo, si no entiendes qué te ofrece la página web para descargar, no aceptes el contenido.

Esta es la clave para conseguir una protección eficaz. Procura leer a fondo qué es lo que vas a almacenar en tu dispositivo, busca información al respecto y actúa en consecuencia. En caso de que certifiques que estás frente a una amenaza, abandona el sitio web.

Junta de Andalucía

Agencia Digital de Andalucía

A continuación te facilitamos algunas pautas adicionales para que gestiones tus archivos descargados de forma segura y responsable.

¿Cómo actuar frente a las descargas?

Existen todo tipo de sitios web de descargas en los que acceder a una amplia variedad de archivos. Películas, videojuegos, libros o canciones son algunos de los ejemplos más habituales. **Si bien no tendrás problemas para encontrar una página que cumpla la ley, existen sitios en los que es posible realizar una descarga ilegal de contenidos**. Es en estos espacios donde hay que extremar las precauciones.

Para empezar, **procura no visitarlos ni descargar ninguno de los archivos que ofrecen**. No solo estarías cometiendo un delito al descargar una película pirata, por ejemplo, sino que también se podría generar una brecha en la seguridad de tu ordenador. Los propietarios del sitio web podrían insertar programas maliciosos o un virus informático, como es el caso de un troyano, en los archivos.

Además, mientras permanezcas en estas páginas, irán abriéndose ventanas automáticamente. Estos *pop-ups* o ventanas emergentes **suponen un riesgo real, ya que algunas descargan información en tu ordenador sin pedir permiso ni avisar**. Por tanto, evitar este tipo de sitios web es una medida muy efectiva de ciberseguridad.

Además de esto, también puedes **configurar tu navegador para que bloquee cualquier ventana emergente que aparezca**. Esto no solo mejora el rendimiento del ordenador y reduce las molestias que provocan, sino que impide las descargas no deseadas.

El funcionamiento de estas herramientas es muy eficiente, ya que frenan su aparición por completo. Es una forma simple y sencilla de aumentar tu seguridad.

Errores frecuentes que debes evitar

Existen diferentes errores frecuentes que debes conocer para poder evitarlos en la medida de lo posible.

Clicar en enlaces poco fiables

Es frecuente clicar enlaces en páginas de terceros o un anuncio de dudosa procedencia. Estos **pueden llegar a tu pantalla a través de un correo electrónico o aparecer en una web**. Por regla general, están pensados para iniciar la descarga de un archivo o para conducirte a un lugar donde efectuarla. Es preciso que no sigas los *links* de este tipo, ya que podrían llevarte a una estafa o a la instalación de programas maliciosos en tus equipos.

Recuerda mantener el sentido común y no descargar un archivo que no entiendas o del que desconozcas su origen. También podrías recibir mensajes con enlaces de este tipo a través de redes sociales. En este caso, no dudes en bloquear a la cuenta que te ha contactado. De esta manera, no podrá seguir enviándote contenido que no te interesa y que potencialmente puede causar daños.

Utilizar aplicaciones gratuitas de origen dudoso

Puedes encontrar una amplia variedad de aplicaciones de uso gratuito. **La mayoría son pruebas de algunas funcionalidades de un programa concreto**. Un buen ejemplo son los antivirus, los cuales suelen ofrecer una protección básica sin coste, que puedes mejorar según tus necesidades. Si bien su funcionamiento es lícito y eficaz, podrías encontrarte con programas maliciosos.

Presta especial atención a aquellos programas que se encarguen de tareas sensibles, ya que pueden suponer una amenaza, por ejemplo en el caso de usar una VPN privada. Se trata de un programa que te permite acceder a una red privada, algo útil para navegar con seguridad y de forma anónima.

Al poder afectar a tu privacidad y bienestar en Internet, procura no emplear productos gratuitos y de procedencia dudosa para este tipo de funciones. Podrían resultar en un acceso indebido a tu ordenador.

No disponer de programas de seguridad

Los antivirus son una defensa excepcional para evitar descargas potencialmente dañinas. Estos se encargan de analizar el fichero en busca de irregularidades y lo ponen en cuarentena si detectan algún problema. De hecho, llegan a impedir el acceso a las páginas de origen si estas no son suficientemente seguras. Además, te impiden abrir el archivo por despiste.

Su funcionamiento suele ser muy bueno, pero **en ocasiones se dan falsos positivos**. Suceden cuando adquieres un programa en una página legal y no sospechosa. El antivirus detecta algún problema y evita que accedas al archivo en cuestión. Es por esto que lo mejor es tener muy en cuenta la página o plataforma en la que realizas la descarga, ya que es un indicador fiable de que no habrá problemas.

Mantener los programas, aplicaciones y navegadores desactualizados

Cualquier programa o aplicación desactualizada se puede convertir en una fuente de problemas. **Los desarrolladores las actualizan para reforzar su seguridad frente a nuevas amenazas**, así como para mejorar su funcionamiento. Por tanto, si no las mantienes al día, no detectarán posibles amenazas al efectuar una descarga. Al no estar preparados, no podrán reconocer los peligros que encierra el archivo.

Esto **también se extiende a los navegadores, cuyo funcionamiento no será el óptimo**. No te impedirán entrar en páginas inseguras, ya que no reconocerán las faltas de seguridad. Por suerte, evitar este error es tan simple como mantener actualizados los programas y aplicaciones que utilices. No te llevará mucho tiempo, pero te ahorrará más de un disgusto a largo plazo.

¿Cómo llevar a cabo una descarga segura?

Lo primero que debes tener en cuenta es dónde vas a realizar la descarga. **Recurre siempre a los sitios del fabricante o páginas de terceros que sean seguras**. Por ejemplo, en el caso de un videojuego, puedes adquirirlo del propio desarrollador o a través de una tienda en línea. Esta es la manera más sencilla de evitar tu exposición a una amenaza. Si optas por piratearlo, tu exposición será mayor y puedes acabar enfrentándote a un problema de seguridad digital.

En caso de que desconfíes del archivo, no dudes en emplear un antivirus para analizarlo. Esta acción es especialmente recomendable en **archivos comprimidos**. El problema en estos últimos reside en que pueden contener programas maliciosos en su interior junto a otros que son inocuos. Al descomprimirlos, la amenaza tiene la posibilidad de instalarse en tu ordenador.

Por último, **evita abrir ficheros sospechosos o descargar archivos adjuntos desconocidos**. En situaciones como esta, es recomendable eliminarlos. Para asegurarte utiliza antes el antivirus, pero si la duda persiste, envíalos a la papelera de reciclaje. Así, evitarás poner en riesgo el contenido de tu dispositivo.

¿Qué medidas preventivas puedes usar?

Tienes a tu alcance una amplia variedad de medidas preventivas para garantizar tu seguridad. Para empezar, **recurre a las versiones de prueba de los programas**. Si tienes alguna duda de su comportamiento o de si este puede resultar peligroso, esta versión te permitirá evaluarlo con una exposición mínima. Luego podrás decidir si te convence o no de acuerdo con tu experiencia.

- **Estudia a fondo la información que te ofrecen en la página web acerca del archivo**. Esto te permitirá saber si te están engañando o no. Los comentarios de otras personas te resultarán de ayuda, ya que no dudarán en contar una mala experiencia. Son una advertencia de los posibles riesgos a la hora de llevar a cabo la descarga. Aunque si dudas de la legalidad del sitio, sal inmediatamente.
- **Protege tus dispositivos móviles**, un detalle al que muchas personas no prestan atención. También puedes descargar archivos en ellos, los cuales están expuestos a los mismos riesgos que un ordenador. Sin embargo, es común ver teléfonos o *tablets* sin antivirus ni protección de ningún tipo, lo que permite a los programas maliciosos infectarlos y luego extenderse a otros aparatos conectados.
- **No dejes de controlar activamente lo que descargas y ten especial cuidado con los menores de la casa**. Asegúrate de explicar los riesgos que pueden existir, ya que su falta de conocimiento podría hacer que acaben cayendo en alguna amenaza. Por ejemplo, podrían acudir a una web fraudulenta pensando que les regalan un videojuego y acabar descargando un virus al ordenador. Por tanto, vigila que no se metan en problemas en un entorno tan amplio como es Internet.

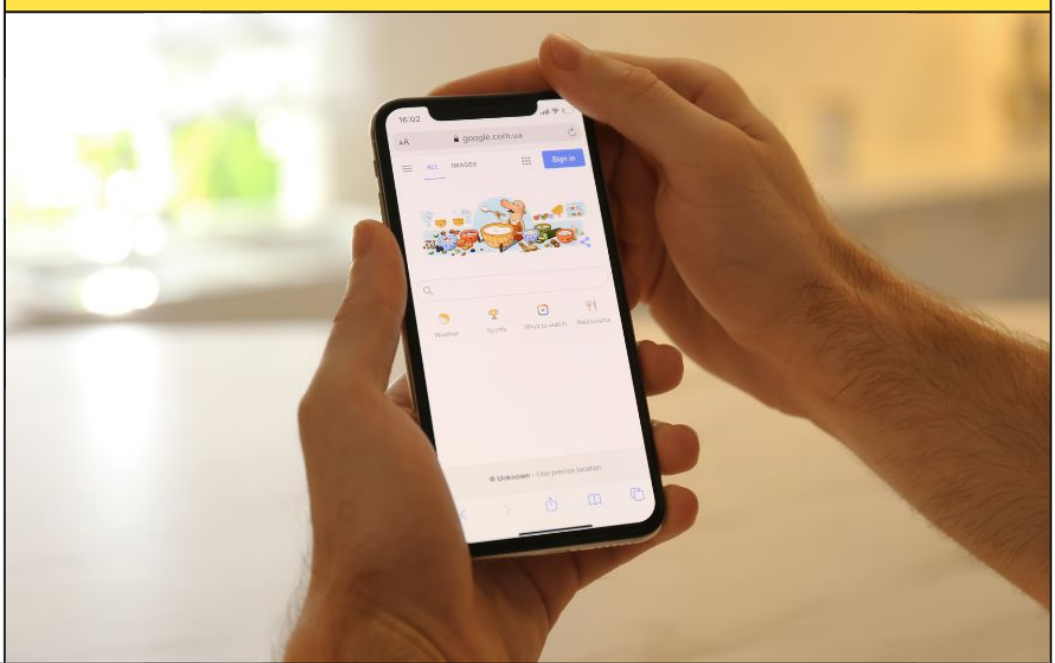
En definitiva, controlar las **descargas** que llevas a cabo es importante para mantener una buena ciberseguridad. Pese a que la mayoría de plataformas son seguras, no olvides actuar de forma precavida. Desconfía si no demuestran qué medidas de seguridad utilizan, recurre al antivirus y elimina los ficheros sospechosos.

vuela

2.5

Borrar toda tu información personal de Google: derecho al olvido

Internet ha supuesto una completa revolución en nuestra forma de relacionarnos con el mundo. Es una herramienta inigualable a día de hoy. En buscadores como Google podemos encontrar datos relevantes sobre cualquier tema, e incluso sobre cualquier persona. Esto último ha provocado complicados debates y también ha despertado preocupación en aquellas **personas que temen que su información privada quede expuesta en la red.** Afortunadamente, en la mayoría de los casos basta con usar el **sentido común antes de publicar o compartir datos** personales para evitar problemas. ¿Y para aquella información que ya está disponible en la red? A continuación, te explicamos cómo ejercer tu derecho al olvido y **cómo borrar toda tu información personal de Google paso a paso.**



Junta de Andalucía

Agencia Digital de Andalucía

El derecho a la privacidad y Google

Resulta muy sencillo **encontrar información** en Internet sobre cualquier persona reconocida, como actores o actrices, personalidades del mundo de la política, de la literatura o **incluso personas anónimas**. Esto hace que a veces sea necesario un esfuerzo extra para **resguardar nuestra intimidad en la red.** En respuesta a esta situación, las políticas de privacidad de Google se han adaptado a las necesidades de los internautas para **garantizar su privacidad** y permitir que cualquier persona interesada pueda solicitar la retirada de información personal de su buscador.

De esta manera, cualquiera que lo solicite tiene derecho a que sus datos personales no aparezcan de forma pública. Es una posibilidad a tener en cuenta por ejemplo de cara a la **búsqueda de un nuevo trabajo**, o incluso para controlar de forma periódica la información personal que aparece en Internet. Para saber si debemos solicitar la retirada de información, es interesante averiguar primero cuál es la **huella digital** que hemos dejado en Internet.

¿Qué es la huella digital? ¿Cómo accedo a ella?

Se entiende por huella digital todo el **rastro que una persona deja al navegar por Internet.** Esta se compone de todos los datos públicos, tanto los que compartimos de forma directa, como los que facilitan otras personas sobre nosotros. Hasta ahora, solo podíamos controlar los primeros. No obstante, ahora podemos pedir a Google que elimine la información que también otras personas han publicado sobre nosotros para que no aparezca en los resultados de búsqueda.

Normalmente, la huella digital la suelen utilizar las empresas para **crear perfiles para sus campañas de marketing**. De esta manera, las empresas encuentran a quienes tienen potencial de consumir sus productos o servicios y pueden enviarles información, o filtrar la **publicidad** de acuerdo a parámetros demográficos y geográficos para que solo aparezca a grupos de personas determinados. En otras ocasiones, son las empresas de recursos humanos las que utilizan la huella digital para conocer mejor a las personas candidatas a sus ofertas de empleo. No obstante, en el peor de los casos, es posible que los y las **ciberdelincuentes** traten de aprovechar tu información privada para realizar ciberataques.

Para descubrir cuál es tu huella digital, debes **buscar tu nombre y tus apellidos en Google**. Búscalos de distintas maneras, y junto a otros términos que consideres que puedan ir asociados con tus datos personales. Si encuentras algo que no quieras que aparezca en el buscador de Google, a continuación te explicamos **cómo eliminar tu información personal de Internet**.

Cómo solicitar a Google que retire información de su buscador

Tras haber averiguado cuál es tu huella digital, puede que quieras **eliminar la información** que el buscador de Google tiene sobre ti. Lo primero que puedes hacer es **contactar directamente con la compañía**, puesto que cuenta con un área específica para encargarse de la **protección de datos** de las personas usuarias.

El enlace al que se debe acceder es este, donde se encuentra el **formulario para solicitar la retirada de información personal**. En él, la propia compañía te explica que estás en tu derecho de solicitar que ciertos datos personales relacionados contigo desaparezcan de los buscadores. Esto es lo que se conoce como **derecho al olvido**.

Tendrás que rellenar un pequeño cuestionario para que Google sepa exactamente qué debe eliminar. Además, si ya has presentado la solicitud anteriormente, podrás indicarlo. Tras esto, tendrás que adjuntar las direcciones de los sitios web en las que aparece la información que quieres eliminar. Es por eso que es importante que busques antes tu huella digital, y que **recopiles aquellas páginas en las que consideras que hay contenido que no debería ser público**. Además, debes indicar también cuál es el motivo de la eliminación. ¿Por qué consideras que se vulnera tu derecho a la privacidad? Normalmente, bastará con que lo indiques de forma breve.

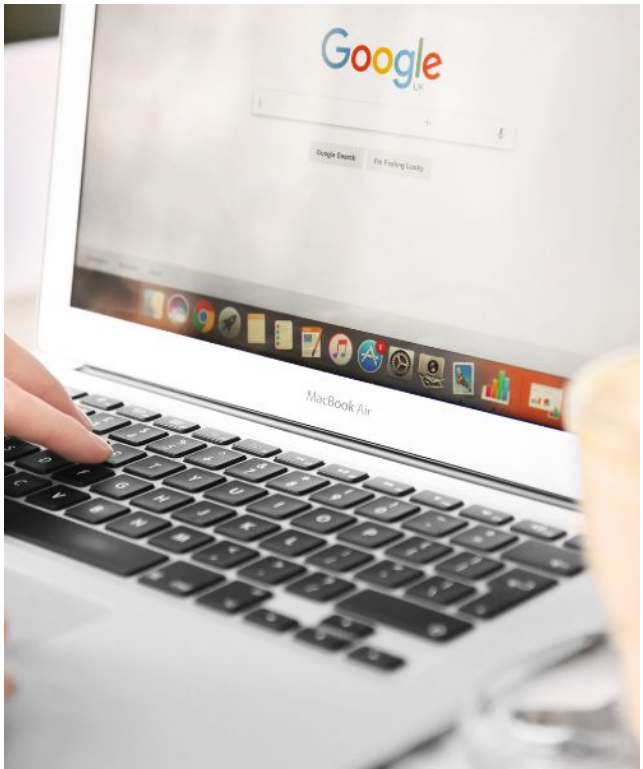
Por último, se te pedirá también que adjuntes el nombre que has utilizado para realizar las búsquedas, y que firmes la solicitud. Si lo que quieres hacer es retirar tus datos de otros servicios de Google, como el buscador de imágenes o YouTube, tendrás que acceder a este otro formulario. Como en el caso anterior, tendrás que **indicar la dirección de la web y el motivo por el que quieres borrar esos contenidos.**

No siempre funciona, por desgracia

Este formulario no funciona en todo el mundo. Solo se aplica en las **versiones europeas del navegador**, con lo cual tus datos podrían continuar apareciendo en las versiones internacionales de los sitios web.

No solo eso, sino que **habrá solicitudes que Google no acepte**. ¿En qué se basa la compañía para aceptar unas peticiones y no otras?

- Si los datos sobre tu vida privada han quedado **obsoletos** y no ponen en riesgo tu privacidad actual, probablemente no los borre.
- Si esta información se presupone de **interés público**, continuará estando disponible. Tampoco la eliminará si guarda relación con estafas financieras, con condenas penales o con tu conducta como persona funcionaria.

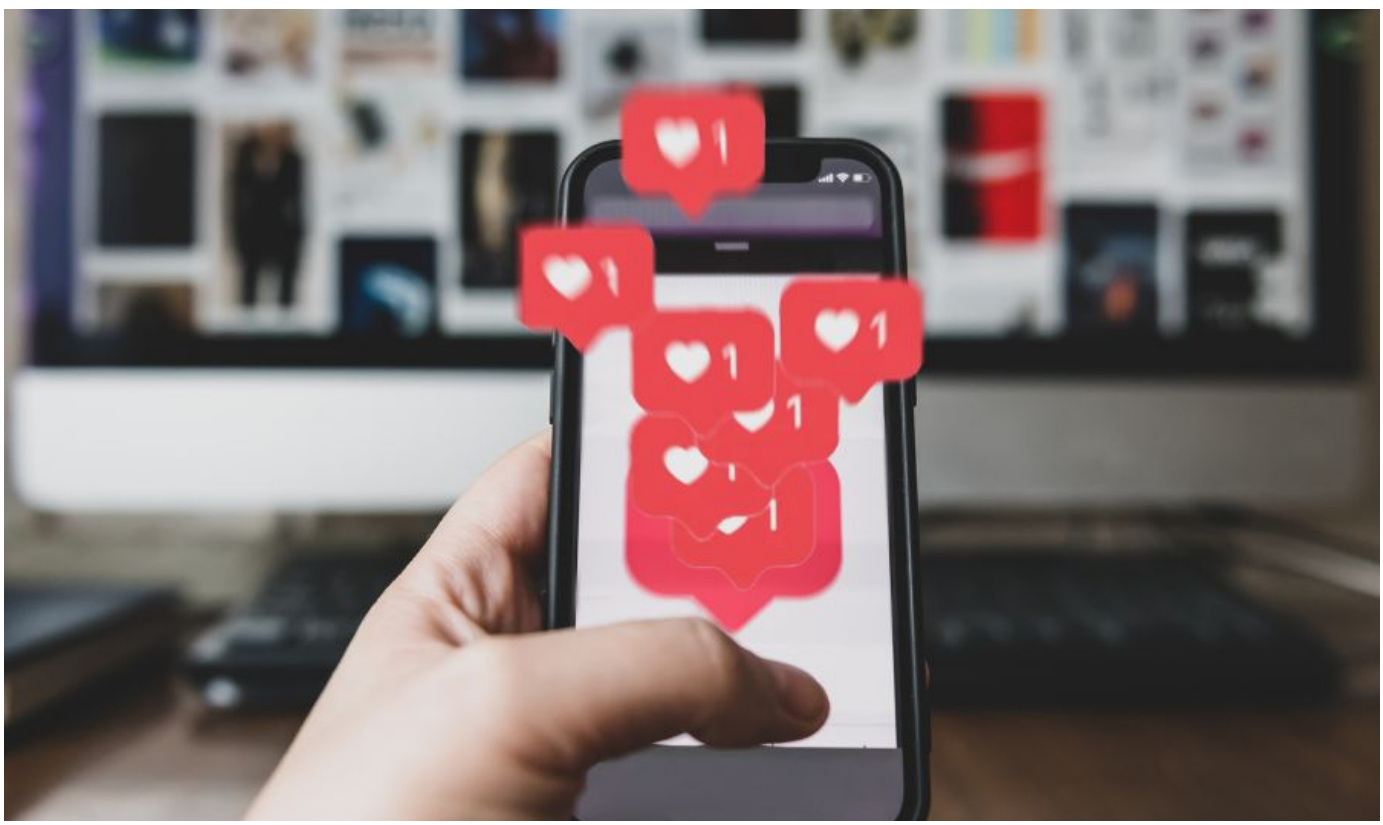


Ejerce tu derecho al olvido: las redes sociales

Además de enviar un formulario a Google, hay **otras medidas** que puedes tomar para garantizar el derecho al olvido. Como, por ejemplo, borrar tus redes sociales o, al menos, la información sensible que almacenas en ellas.

Si en tus **redes sociales** aparecen tu nombre y tus apellidos, cuando te busquen podrán encontrarte rápidamente. Es importante que seas consciente de esto en todo momento, y solo publiques aquello que realmente sientas que puedes compartir sin problema. Es decir: **no reveles información privada**, ni cualquier dato que quieras mantener lejos del conocimiento público.

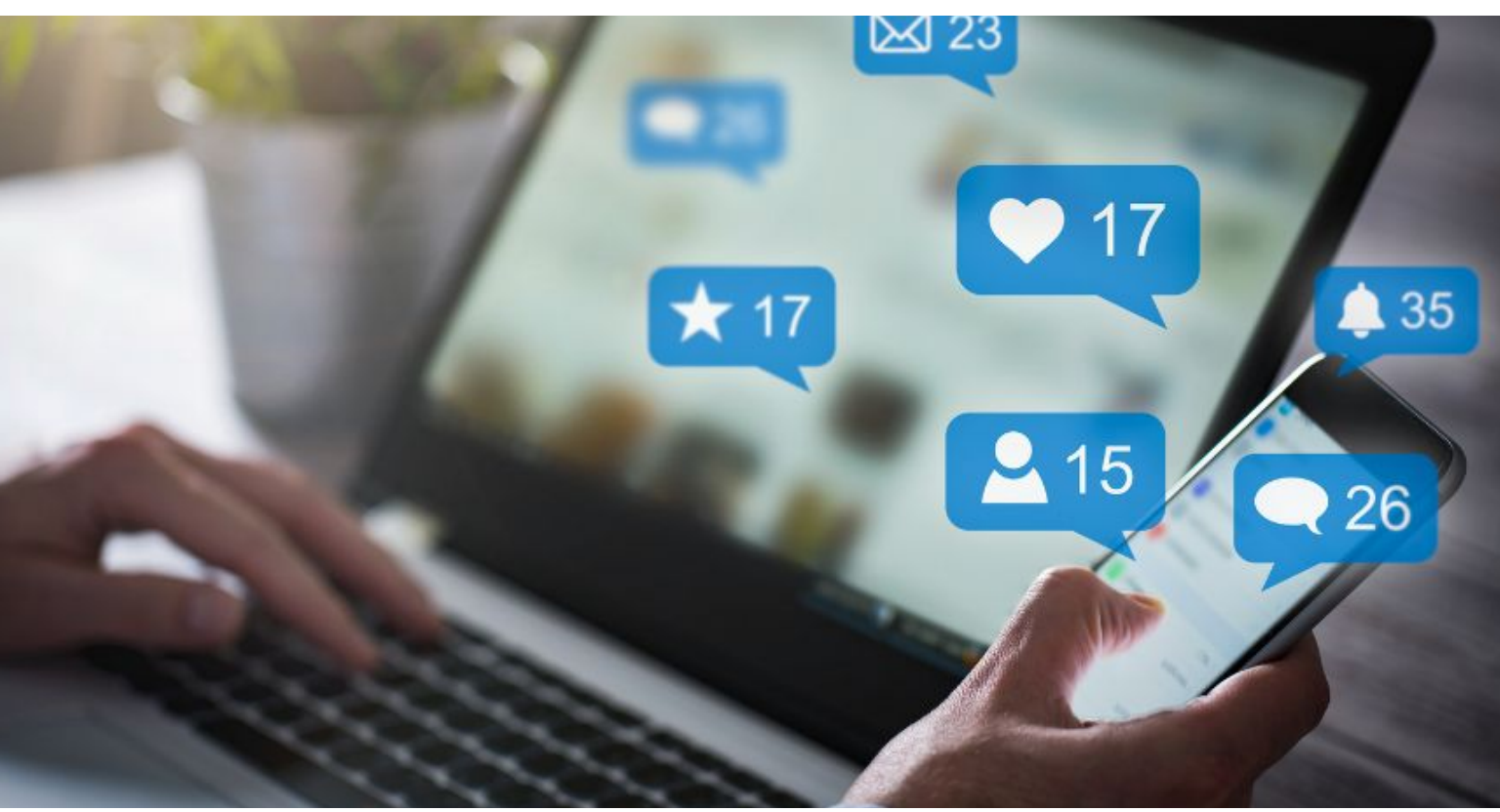
Puedes optar por **cambiar los nombres de tus redes sociales**, y usar algún tipo de **seudónimo**. De esta forma te aseguras de que solo te encuentren las personas a las que se lo hayas facilitado, y no cualquiera que sepa tu nombre y apellidos. Pero si lo que quieres es eliminar o controlar la información personal que compartes en la actualidad, te enseñamos cómo hacerlo en algunas de las redes más conocidas.



Comencemos por **Facebook**, red en la que mucha gente comparte contenido personal casi sin darse cuenta. Deberás **acudir a tu perfil** y señalar qué datos quieres que aparezcan y, sobre todo, cuál de toda esta **información quieres que sea pública y cuál privada**. Recuerda que también puedes seleccionar **quién tiene permiso para etiquetarte** en sus fotos, así como las imágenes que quieres que aparezcan en tu perfil.

Por otro lado, tenemos **Instagram**, donde se suele transmitir menos información en el perfil, pero mucha más en las publicaciones. **Vigila el contenido** de estas, así como el que comparten tus amistades o familiares, y no admitas etiquetas si no te gusta lo que aparece en la fotografía o se deduce de ella. También puedes acudir a tu perfil y modificar aquello que dice de ti o incluso dejar este apartado en blanco.

En el caso de **X** (anteriormente Twitter) también es bastante sencillo, puesto que solo tendrás que acudir al botón de **editar perfil** para ver qué datos compartes. Esta red social cuenta con un **formulario específico** para denunciar la divulgación de información privada, que podrás usar siempre que sientas tus derechos vulnerados.



¿Por qué alguien pediría la retirada de información personal de Internet?

El proceso de **eliminar información personal de Internet** no es complejo, pero sí puede resultar tedioso. Por eso, lo mejor es **controlar desde el primer momento qué compartimos** en las distintas redes, así como lo que se publica de nosotros. No obstante, cuando se es un personaje público puede llegar a ser mucho más complicado. Siguiendo los pasos que hemos descrito anteriormente, podrás **borrar toda tu información personal de Google** y ejercer tu derecho al olvido con bastante facilidad.

Son muchos y variados los motivos que pueden llevar a una persona a solicitar que desaparezcan sus datos del buscador. El primero y fundamental es que tiene **derecho a la protección de sus datos**, y es un derecho que puede ejercer libremente. Pero además de este, pueden darse casos más complejos. Por ejemplo, puede aparecer una noticia en un medio digital donde se aporte tu nombre asociado a alguna actividad que no hayas realizado. Si te perjudica, y el medio no responde a tus intentos de corregir la información, Google actuará por ti.

Aunque normalmente esta situación de querer retirar la información se está dando principalmente entre población joven que busca acceder a su primer trabajo, o mejorar en el ámbito laboral. Las empresas pueden llegar a realizar búsquedas sobre las personas que optan a sus puestos de trabajo, y para **evitar que se encuentre información del pasado** que no encaje con el perfil actual de la persona, se opta por eliminarla. Aunque lo ideal es cuidar siempre aquello que se publica, en plena adolescencia o juventud esto puede ser bastante complicado. De ahí la necesidad de que empresas como Google permitan eliminar los datos, de modo que garanticen el tan importante derecho al olvido.

Internet es una herramienta de enorme potencial, que facilita el acceso a una gran cantidad de información que antes no estaba disponible para todo el mundo. Por ello es imprescindible aprender algunas pautas básicas de seguridad que nos permitan navegar de forma respetuosa y segura. Ahora que ya sabes **cómo borrar toda tu información personal de Google**, recuerda que en nuestra web **encontrarás todas las claves** para manejarte con confianza en este nuevo mundo digital.

vuela

2.6

Recomendaciones para mejorar tu privacidad: las claves importantes

Una de las formas más sencillas de mejorar tu seguridad digital al navegar por Internet consiste en **cuidar la privacidad de los datos y archivos que compartes.** En la actualidad, **la información que se vierte en la red es abrumadora**. A lo largo de un solo minuto, se envían 60.000 mensajes en WhatsApp, se comparten 650.000 historias en Instagram y se suben a YouTube 500 horas de vídeo. Y todo esto es posible gracias a que las personas internautas reciben y generan contenido de forma continua.

Entre tanto contenido, es posible que a veces se incluyan datos que normalmente no querríamos compartir. Para **evitar que subas a la red información personal o sensible** acerca de ti, es importante que tengas en cuenta algunas pautas. ¿Te gustaría descubrirlas?

Junta de Andalucía

Agencia Digital de Andalucía

¿Por qué cuidar tu información personal?

Antes de empezar, ten claro una cosa: la red es un lugar seguro. **Gran parte de los sitios web cuentan con medidas de seguridad eficaces para evitar filtraciones de tu información personal**. Por ejemplo, siempre te pedirán permiso para utilizar datos concretos, los cuales podrás revisar en las políticas de privacidad de cada sitio. Además, la legislación actual protege a las personas usuarias de Internet de un uso fraudulento o inadecuado de sus datos personales.

No obstante, tú también **puedes y debes proteger activamente tu información personal de quedar expuesta**. Podrías caer en un despiste y publicar datos comprometedores que otras personas podrían emplear en su beneficio o para hacerte daño. Esta es la principal amenaza que existe en la red, de la cual hay que cuidarse actuando de forma precavida y responsable.

Clasificación de datos personales

Los primeros datos a considerar son los de contacto. En estos se incluyen los referentes a tu **domicilio, correo electrónico o teléfono**. Procura entregarlos solo a plataformas de máxima confianza y que certifiquen que únicamente los utilizarán para fines comerciales, como entregar un pedido *online*, o para identificarte. Además, evita mostrarlos en las redes sociales o en foros públicos.

Divulgar algunas señas identificativas, como tu nombre, estado civil o lugar de nacimiento, no tiene por qué resultar peligroso. Al fin y al cabo, indicas tu nombre y apellidos en la mayoría de redes sociales, aunque **eres libre de emplear el seudónimo que prefieras**. Sin embargo, ten **especial cuidado con dar a conocer tu firma electrónica** y más información de la necesaria. En caso de que sientas inseguridad, no dejes de **configurar tus perfiles en modo privado** para prohibir su visionado por parte de otras personas más allá de tus contactos.

También es frecuente publicar referencias académicas o laborales, e incluso existen plataformas destinadas a estas labores, como es el caso de LinkedIn. Son útiles a la hora de buscar trabajo o conocer otras personas con intereses similares. Por otro lado, **las informaciones acerca de tu patrimonio, como propiedades que puedas poseer o tus ingresos, no te aconsejamos publicarlas**, ya que quienes delinquen se sentirían atraídos por ellas y podrían señalarte como su próximo objetivo.

Junto a estos, existen datos que se consideran sensibles y **que podrían llevar a discriminaciones o situaciones de acoso**. Este es el caso de la información relacionada con tu **ideología, vida sexual o similares**. Por sí solos, son capaces de dar inicio a conflictos con determinadas personas, algo que facilita el anonimato que reina en la red.

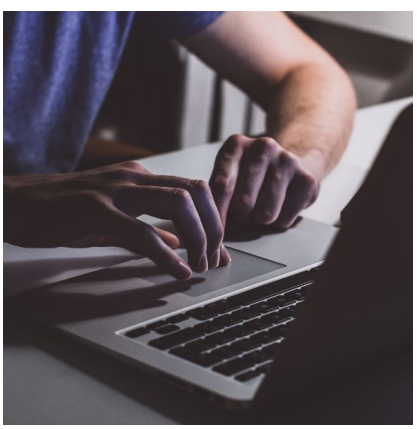
¿Cómo te afecta de forma negativa la publicación de tus datos en la red?

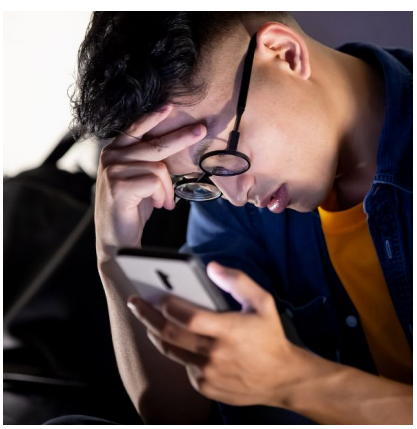
La información que divulgas en la red puede afectarte de manera negativa de diferentes maneras. Recuerda que, **aunque es muy probable que no pase nada, siempre es recomendable establecer las medidas de seguridad necesarias**. De este modo, reducirás al mínimo cualquier posible riesgo. Esto es importante, ya que es mucho más sencillo evitar la publicación de un dato sensible que su eliminación posterior.

Por ejemplo, si elaboras una publicación con una fotografía comprometida y la compartes en la red, esta llegará a tus contactos, quienes podrían compartirla y aumentar el grado de difusión. Así, alcanzarías a personas desconocidas y que tienen en su mano seguir distribuyendo lo que les ha llegado.

Algunas publicaciones podrían traer consigo **consecuencias negativas** que podrían afectarte de forma directa o indirecta. Ten en cuenta estas:

- **Comentarios negativos**. Es una de las consecuencias más comunes. Puede que no tengan mayor relevancia y que no sean especialmente dolorosos. Sin embargo, al realizar una publicación determinada podrían darse insultos o amenazas, sobre todo si está relacionada con algún tema en el que exista una fuerte polarización.
- **Ciberacoso**. Cuando los comentarios negativos no cesan, aumentan en intensidad y comienzan a llegar por canales privados, estás frente a una situación de acoso. Es importante que denuncies tu caso ante las Fuerzas y Cuerpos de Seguridad del Estado, quienes están presentes en las redes sociales. También puedes ponerte en contacto con el INCIBE (Instituto Nacional de Ciberseguridad) en busca de ayuda.
- **Propagación de noticias falsas**. Con tus datos es posible crear noticias falsas, las cuales estarían pensadas para dañar tu imagen o difundir bulos acerca de tu persona.
- **Ataques a tu reputación**. Ligada con la anterior, los datos que publiques, en especial fotos inapropiadas, pueden ser una fuente de ataques hacia tu reputación. Además, cabe la posibilidad de que sean utilizados en tu contra para chantajearte a ti o a tus familiares. Ante esta situación, no dejes de ponerte en contacto con las Fuerzas de Seguridad del Estado o con los sistemas de asistencia de la plataforma que estés empleando.





Consejos para proteger tus datos

Las consecuencias de verter tus datos personales o información en la red varían en gravedad. **Recuerda: eres la primera línea de defensa contra la publicación de tu información más sensible**. Aunque cuentas con la protección de las plataformas que emplees y de las autoridades, es importante que actúes siempre de forma consciente y responsable. Así, navegarás sin problemas para disfrutar de todo lo que te ofrece Internet.

Actúa con precaución

La precaución es la herramienta fundamental para evitar la difusión descontrolada de tus datos personales. Puedes utilizar un alias, colocar tus cuentas en privado, no mencionar información propia que sea de interés o cuidar las fotografías que compartes. Dispones de una amplia variedad de opciones para **protegerte de manera activa**.

Tampoco des información personal en páginas que no sean seguras. **Los navegadores te informarán cuando estas no cuenten con los certificados apropiados**. Ten en cuenta que estos sitios podrían estar destinados a actos maliciosos. Un buen ejemplo es la práctica del *phishing*, en la que las y los ciberdelincuentes clonarán la web de una institución o una tienda para tratar de obtener datos relevantes de quienes la visiten.

No instales aplicaciones innecesarias

Si instalas aplicaciones innecesarias, estarás exponiendo tus datos. Tendrás que registrarte en ellas y, en caso de usar un dispositivo móvil, te pedirán el control temporal sobre diferentes áreas, como la cámara o el micrófono. Para aumentar tu seguridad, procura usar solo aquellas aplicaciones que realmente necesites y desinstala el resto.

Además, **antes de eliminar una aplicación recuerda borrar primero el perfil que has creado para poder usarla.** Esto llevará al personal responsable a deshacerse de la información que guardase acerca de ti. Así, evitas una posible fuga de información por un ataque informático a la empresa.

Bloquear *cookies*

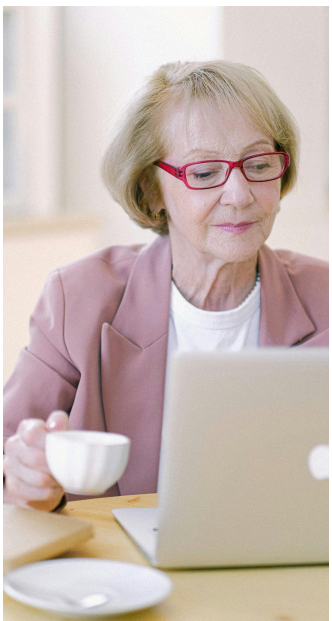
Bloquear las *cookies* es una forma eficaz de no dar algunos datos a las páginas web que visitas. Son un tipo de fichero empleado para recordar tus accesos y conocer tus hábitos de navegación. Dan información sobre cómo te comportas en la web, que se emplea por ejemplo para proponerte ofertas personalizadas. También son útiles para acceder rápidamente a tus cuentas, ya que pueden guardar tus contraseñas.

Gracias a normas como el RGPD, tienes un gran control sobre las *cookies*. **Las páginas te avisan de su uso cuando accedes y puedes tanto rechazarlas como aceptar las que tú quieras**. Además, te dan la opción de elegir cuáles permites usar a la web y las que no.

Protección anti-rastreo

Los navegadores, como Chrome o Firefox, cuentan con opciones de protección anti-rastreo. Su objetivo es aumentar tu seguridad y privacidad durante tu navegación. Para ello, estas herramientas evitan que se guarde información sobre tus búsquedas, así como que recibas un exceso de publicidad no deseada (*spam*).

También te ayudan a protegerte contra programas maliciosos, rastreadores en las redes sociales o las *cookies* de terceros. **Otra opción interesante que te permite no dejar huella es la navegación en modo incógnito**. Con ella no enviarás ningún dato acerca de tu comportamiento, por lo que no verás **anuncios personalizados** ni podrán saber quién eres. En definitiva, siguiendo estas **recomendaciones para mejorar tu privacidad** disfrutarás de una navegación más segura. Recuerda protegerte activamente y presta atención a las medidas de seguridad de los sitios web que visitas.



vuela

2.7

Sitio web seguro: maneras de determinar si estás en uno de ellos

Un sitio web seguro te garantiza una navegación sin problemas. Si bien la inmensa mayoría de páginas son seguras, algunas no cuentan con medidas específicas para protegerte, por lo que será mejor evitarlas para mantener la seguridad de tus dispositivos y de la información privada que almacenas en ellos.

Como podrás ver, aprender a identificar un sitio web seguro es muy importante. ¿Sabes por dónde empezar? Te facilitamos todas las herramientas que necesitas. ¡Acompáñanos!

Junta de Andalucía

Agencia Digital de Andalucía

¿Cómo puedes verificar si un sitio web es seguro?

Existen diferentes factores que te permiten **identificar un sitio web seguro**. **Uno de ellos es la propia URL o dirección de la página**. Los estándares de seguridad actuales, como el SSL (*secure sockets layer* o capa de espacios seguros), modifican una parte, la cual puedes utilizar a modo de verificador. Solo tienes que clicar en la dirección que aparece en la barra de búsqueda del navegador y fijarte si empieza por «https». Si es así, estarás accediendo a un lugar seguro con la garantía de tener tus datos protegidos. En caso de que empiece por «http», sin la «s» (de seguro), no lo estarán.

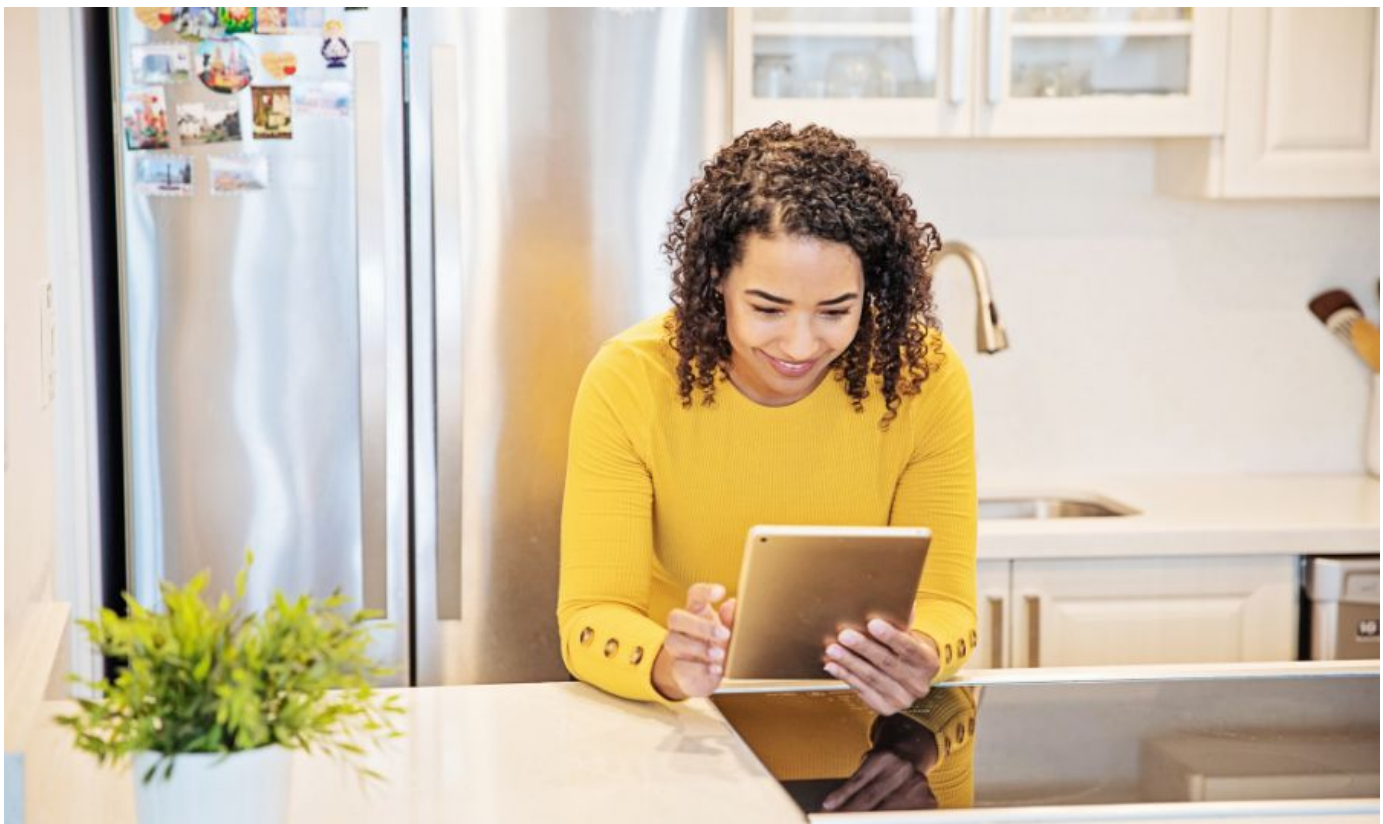
Además, **presta atención a que la dirección esté escrita correctamente**, ya que podrías acabar en una página web alternativa. En ocasiones, las personas ciberdelincuentes crean páginas web con la intención de suplantar la identidad en Internet de una marca o empresa. Si bien en la mayoría de casos las empresas adquieren diferentes dominios relacionados con su nombre, no está de más que revises si es la correcta o no.

Otra alternativa para comprobar la seguridad sigue estando en la propia barra de búsquedas. **Presta atención al lado izquierdo, cerca de la dirección verás un candado que debería permanecer cerrado**. En caso afirmativo, el portal web es seguro, ya que usa un **certificado** SSL. En caso de que sea insegura, aparecerá un triángulo rojo con una exclamación.

Además de todas estas indicaciones, existen otros factores que puedes verificar. Uno de ellos es la **existencia de publicidad agresiva o ventanas emergentes insistentes**. Estas no dejarán de aparecer y tratar de captar tu atención. También es común que aparezcan **solicitudes de información sospechosas**, que te piden datos personales o acceso a tu ordenador.

Junto a esto, **las páginas fraudulentas suelen contener faltas de ortografía evidentes**, descuentos que no tienen sentido o remedios milagrosos. Su **diseño está habitualmente poco cuidado** y encontrarás enlaces que no conducen a ningún lado. Si identificas varios de los indicadores mencionados, es recomendable que abandones la web.

Busca la política de privacidad del sitio web. Este es un síntoma de que estás en una página de confianza, ya que en este documento el propietario te explica la actividad que realiza o cómo se usan tus datos. No dudes en consultarla y verificar la información que aparezca en ella, al fin y al cabo te afecta directamente como persona usuaria de sus servicios. En esta parte de la web también **puedes cotejar los datos del propietario**, que aparecerán en su interior, para verificar que es realmente quien dice ser.

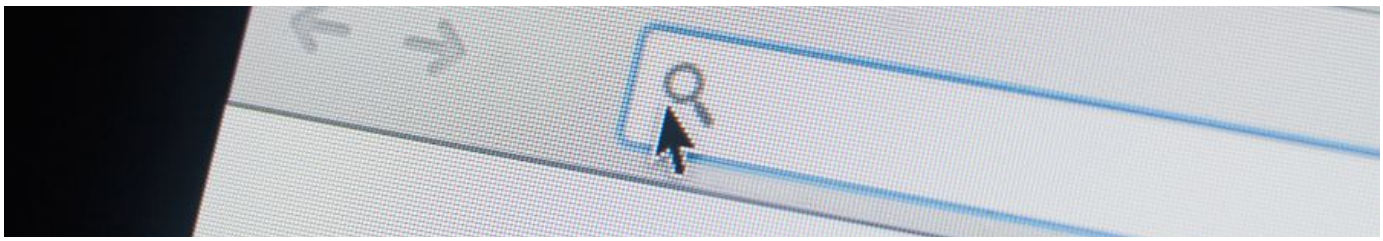


Otros modos de verificación

Por regla general, **los sitios web muestran los métodos para contactar con la persona propietaria**. Estos se encuentran en la propia página de contacto, en la parte baja de cada sección o en la zona alta. Ya sea a través de correo electrónico o teléfono, si tienes alguna duda acerca de la seguridad, no dejes de realizar la consulta. De esta forma, te aseguras de que existe una persona responsable capaz de responder a tus preguntas.

Una señal de peligro se basa en los redireccionamientos maliciosos, los cuales te conducen a otra web en cuanto accedes a la primera. Esto podría ocurrir en una página segura, en especial en las conocidas como páginas de aterrizaje. Sin embargo, si encuentras algún factor dudoso, como una oferta exageradamente buena, podría tratarse de un sitio web malicioso.

Los propios motores de búsqueda te avisan antes de acceder a la página de su posible inseguridad. Si vas a acceder a un sitio peligroso, te aparecerá una ventana informándote y preguntándote si quieres seguir adelante. Encontrarás frases como «Visitar este sitio puede ser perjudicial para su equipo«, lo que te servirá de indicación. No obstante, ten en cuenta que estos mensajes no son siempre precisos.



¿Existen herramientas para identificar sitios inseguros?

Por suerte, existen herramientas que te permiten **identificar páginas web fraudulentas** o poco seguras de forma casi automática. **Los propios navegadores cuentan con medidas que las detectan**. Estas consiguen bloquear ventanas emergentes, desactivan contenido inseguro o frenan descargas no autorizadas. Además, puedes comprobar el nivel de seguridad que estás usando con total libertad.

Por ejemplo, si estás utilizando el navegador Chrome de Google, sigue esta ruta: Configuración, Configuración avanzada y Privacidad y Seguridad. En esta sección **podrás borrar las *cookies* de navegación o revisar cuáles son,** ajustar la seguridad o controlar la información a la que pueden acceder los sitios web que visitas. Las opciones que te ofrece son completas y totalmente personalizables. En todos los navegadores podrás encontrar soluciones de seguridad similares dentro de la pestaña de Configuración.

También existen herramientas disponibles en línea para rastrear direcciones en buscas de virus u otras amenazas. **Un ejemplo es VirusTotal, una web que te permite verificar otras**, así como archivos que sospeches que puedan estar infectados. Otra que te interesará es la herramienta **whois** de la Corporación de Internet para la Asignación de Nombres y Números (ICANN). Gracias a ella podrás saber a quién pertenece la web, cuándo la registró y podrás contactar con el o la propietaria.

Por último, hoy día la mayoría de antivirus cuentan con funciones integradas para verificar sitios web.

Como ves, **tienes a tu alcance diferentes alternativas para comprobar que una web es auténtica** e, incluso, conocer quién la posee. Es muy recomendable prestar atención a este detalle, ya que es la clave para saber si es alguien de fiar o no.

¿Por qué debes navegar en sitios seguros?

Cuando navegas por sitios web seguros, estás minimizando el riesgo de que tu equipo quede afectado por un ataque cibernético, como un virus o cualquier otro tipo de programa malicioso diseñado para ocasionar un perjuicio en tu ordenador o teléfono móvil.

También **evitarás ser víctima de fraudes, estafas o robo de datos**. Quienes delinquen suplantan la identidad de páginas seguras con estas finalidades. Esto se conoce como *phishing* y consiste en emplear un anzuelo, en este caso una web, para realizar sus actividades. Podrían hacerse pasar por una tienda en línea y conseguir tu cuenta bancaria o el número de tu tarjeta de crédito sin que fueras consciente de ello. Sin embargo, manteniendo una navegación segura y tomando las precauciones necesarias, como comprobar la veracidad de la página antes de efectuar la compra, evitarás este problema.

Junto a esto, estarás cumpliendo la legalidad, ya que **muchas páginas web inseguras se dedican al pirateo de música, películas o videojuegos**. Al visitar estos sitios es frecuente que los dispositivos queden infectados por todo tipo de programas maliciosos. Las personas propietarias no guardan las medidas de seguridad necesarias, suelen abusar de los anuncios y solicitarán todo tipo de permisos que no debes dar.

Además, en caso de que efectúes una compra, **es posible que luego no puedas contactar con el proveedor**. También perderás la garantía de que el producto llegue en buen estado o que realmente adquieras lo que habías comprado.

¿Por qué apuestan las páginas web por la seguridad?

Los peligros en la red existen, eso es algo innegable. **Esto lleva a que las y los propietarios de los sitios web, en muchas ocasiones empresas de gran renombre, trabajen activamente para protegerte.** De actuar de forma contraria, se estarían saltando la legalidad vigente. Un buen ejemplo es el cumplimiento del RGPD, el cual define cómo tratar tus datos y la protección que debe establecerse para que tu información privada no quede expuesta.

Además, un sitio web inseguro **genera desconfianza en sus clientes o usuarios.** Para evitar estos y otros problemas, se afanan en demostrar que sus sitios son de confianza de diferentes maneras. Por ejemplo, cuando realizas una compra, tendrán un sistema específico para garantizar la seguridad de la compra, del cual siempre te informarán para una mayor tranquilidad.

Una mala seguridad también afecta a la experiencia de la persona usuaria. Si la web no actúa como es debido, se sentirá frustrada e incómoda, lo que le llevará a irse a la competencia. Por tanto, existe un fuerte incentivo a garantizar una correcta navegación en todo momento, desde tu aterrizaje hasta cuando decidas abandonar la página.

En definitiva, navegar a través de **un sitio web seguro** te ayudará significativamente a cuidar de tus dispositivos y de la protección de tu información. En caso de que tengas dudas sobre la seguridad de un sitio web, revisa los factores que hemos expuesto.

vuela

3

Aumenta tu seguridad con las herramientas adecuadas

Fortalece tu protección en línea mediante el uso de herramientas especializadas. En esta sección exploraremos cómo el conocimiento de las amenazas cibernéticas más comunes y la adopción de medidas preventivas adecuadas pueden aumentar significativamente tu seguridad en la red.

Junta de Andalucía

Agencia Digital de Andalucía

vuela

3.1

Virus informático: recomendaciones para utilizar un antivirus

Al igual que cuidas tu salud para protegerte de los virus**, tus dispositivos también necesitan protección frente a los virus informáticos**. De este modo, conseguirás **prevenir o limitar sus daños**. Si mantienes un comportamiento responsable cuando navegas por Internet y cuentas con un buen antivirus, ya estás proporcionando a tus dispositivos una primera línea de defensa frente a la mayoría de riesgos que habitan en la red.

A continuación te mostramos cómo puedes convertir tu antivirus en una solución completa y eficaz de seguridad digital, exprimiendo a fondo todos sus beneficios.

Junta de Andalucía

Agencia Digital de Andalucía

¿Cómo actúa un antivirus para proteger tus dispositivos?

Un antivirus es un *software* integral de seguridad. **Esta herramienta digital se encarga de analizar tu ordenador, *tablet* o teléfono móvil** en busca de virus o archivos infectados que eliminar.

A su vez, y gracias a su evolución en los últimos años, la mayoría de antivirus también son capaces de **detectar la presencia de programas maliciosos o *malware***, programas espías o *spywares* y otras muchas amenazas que se dedican a recopilar información personal o alterar el correcto funcionamiento del equipo.

Además de analizar el equipo en el momento en que se lo indiques o de forma regular, el antivirus te permite **escanear archivos descargados** en tus aparatos y **verificar la seguridad del sitio web que vas a consultar.** En consecuencia, esta herramienta no solo impide que surjan vulnerabilidades, sino que también ayuda a mantener un comportamiento más responsable.

Sin duda, una de las funciones más útiles del antivirus es la posibilidad de **revisar al completo los diferentes archivos presentes en tu disco duro.** Esto es muy útil para garantizar que ninguna amenaza cibernética se ha instalado entre tus archivos o para comprobar si algún sitio web ha realizado una descarga maliciosa sin tu permiso en el equipo.

Este análisis tardará más o menos en función de la cantidad de archivos almacenados en tu dispositivo. Por regla general, puedes **configurar el antivirus para que periódicamente se analicen en profundidad tus archivos de forma automática**. También puedes recurrir a un análisis más breve, que se centrará en comprobar la salud de los principales sistemas, archivos y programas.

Los beneficios de los antivirus

El principal beneficio que te aportan los antivirus es la protección contra los riesgos presentes en Internet. Además, **no solamente te protege a ti, sino que rompe la cadena de transmisión hacia otros dispositivos**. La defensa es eficaz y en la mayoría de las ocasiones es preventiva. Esto quiere decir que el antivirus detectará la amenaza justo cuando trata de acceder al sistema, por lo que te mantiene a salvo sin que te des cuenta.

También **te ofrecen protección frente al *spam* de anuncios no deseados**, que llenan tu pantalla de ventanas emergentes de publicidad. Estas pueden ralentizar el funcionamiento del sistema y perjudicar la navegación. Ten en cuenta que esta práctica no solo se orienta a molestar, sino que en ocasiones se utiliza para tratar de introducir programas maliciosos en el ordenador.

Otra ventaja es que **protegen la seguridad de dispositivos portables, como es el caso de un disco duro externo o una memoria USB**. Al conectarlos a tu ordenador, el antivirus los analizará en busca de amenazas. Esta acción la puedes llevar a cabo personalmente o configurar tu antivirus para que se realice de forma automática.

Peligros frente a los que protege un antivirus

La principal amenaza frente a la que te defienden son los **virus**. Estos programas **se diseñan para entrar sin ser detectados en ordenadores ajenos**. Su objetivo es el de robar archivos, borrar documentos, modificar la configuración o, simplemente, causar molestias. Hay virus de diferentes tipos, por lo que es muy recomendable mantener el equipo preparado.

También se encargan de prevenir la entrada de **gusanos informáticos. Son programas capaces de ejecutarse y propagarse por sí mismos a través de una red**. Cuando se ponen en marcha, se dedican a colapsar las redes y equipos en los que se encuentran. A la hora de expandirse, utilizan correos electrónicos o cualquier otro medio disponible.

Por último, los **troyanos** son otro tipo de amenaza ante la que defienden, la cual es difícil de detectar. **Se ocultan con la apariencia de un programa legítimo** para, una vez ejecutado, permitir el control remoto del equipo en el que se encuentren. El peligro que suponen es alto, ya que otra persona tendrá acceso completo a tu ordenador, con todo lo que esto supone.

¿Cómo elegir un buen antivirus?

En la actualidad puedes disponer de una amplia variedad de programas de seguridad digital de gran calidad completamente gratis. **La mayoría de los desarrolladores ofrecen las funcionalidades básicas, como el análisis del ordenador o teléfono móvil, sin coste alguno**.

Procura escoger un antivirus con una interfaz sencilla. Esto te ayudará a comprender rápidamente el funcionamiento de la herramienta y cómo poner en marcha cada una de sus opciones. Además, sabrás cómo reaccionar siempre que se presente un problema, lo que te facilitará tomar la decisión adecuada.

Junto a esto, **escoge aquel antivirus que cuente con actualizaciones diarias** o en el menor lapso de tiempo posible. Así, conocerá las últimas amenazas que han aparecido y podrá defender tu ordenador de manera efectiva.

Por descontado, **no utilices un programa pirata, ya que estos podrían ser troyanos**. Recuerda que tienes opciones de antivirus gratuitos en sus funciones básicas. Este es el caso de Avira o Avast, los cuales mantendrán alejada cualquier amenaza.

Por su parte, el sistema operativo Windows cuenta con antivirus incorporado: Windows Defender. Este **se encarga de evaluar las posibles amenazas presentes en el ordenador**, evita que entres en páginas inseguras o bloquea una aplicación si esta es sospechosa. Una de sus mayores ventajas reside en que es capaz de trabajar en colaboración con otras aplicaciones del mismo tipo que instales. **Ten en cuenta que muchos antivirus son incompatibles entre sí**, por lo que no puedes instalarlos todos simultáneamente.

Tipos de antivirus

Los antivirus se presentan en tres categorías principales. Cada una está pensada para responder a las necesidades de quien los utiliza, pero todos ellos te ofrecerán una solución efectiva.

- **Antivirus autónomo**. Es un programa **especializado en detectar y analizar virus concretos.** Se instala en un dispositivo portátil, como un USB, y **se emplea en ordenadores ya infectados**. Así, es posible devolver estos equipos a la normalidad de forma sencilla y sin infectar otras máquinas.
- **Paquetes de seguridad**. Son antivirus avanzados que cuentan con **diferentes funcionalidades.** Su base reside en el **análisis de amenazas y su eliminación**, aunque añaden **cortafuegos** (sistemas que impiden el acceso no autorizado), opciones de **control parental o *antispyware***. Este es el tipo de antivirus que más frecuentemente encontramos en nuestros dispositivos.
- **Antivirus en la nube**. En estos casos el antivirus se encuentra alojado en la nube, es decir, en los servidores de la compañía y no en tu ordenador. Únicamente necesitas instalar el cliente (una pequeña aplicación) para poder utilizarlo. **Realizará los escáneres de modo automatizado** y te protegerá en todo momento.

¿Cómo sacarle el máximo partido a un antivirus?

El primer paso que debes seguir es el de mantener actualizado el antivirus. Ten en cuenta que quienes delinquen no dejan de crear amenazas nuevas, por lo que necesitas mantenerte al día. Si no lo haces, estarás poniendo en riesgo tu equipo y el resto de dispositivos. El programa que uses no detectará posibles problemas, ya que no dispone de información para reconocerlos.

Procura programar análisis completos del sistema cada cierto tiempo. Aunque también puedes realizar análisis de forma manual, esta opción es mucho más cómoda. Solo deberás indicar al programa cuándo quieres que entre en acción y, como actúa en segundo plano, podrás dedicarte a otras tareas mientras se realiza el análisis.

Mantén activado el cortafuegos en todo momento. El cortafuegos es un sistema de seguridad que bloquea los accesos no autorizados a un dispositivo. La mayoría de antivirus lo ofrecen de manera gratuita y es una defensa de lo más eficiente. No evita que sigas utilizando una red, pero sí frenará cualquier intento de acceder sin los permisos debidos.

Por descontado, **no cierres el antivirus bajo ningún concepto**. Por suerte, cuando enciendes el ordenador, esta herramienta se pone en marcha de manera automática. Esto evita olvidos o despistes por parte de quien lo está usando. No obstante, podrías llegar a cerrarlo sin darte cuenta o pensando que no lo necesitas. Si haces esto, estarás desprotegido frente a cualquier amenaza de la red.

En definitiva, **la mejor defensa contra la mayoría de ataques informáticos comienza por la instalación de un antivirus.** Estos programas aumentan tu seguridad cuando navegas y protegen tu información frente a los y las ciberdelincuentes.

vuela

3.2

Gestor de contraseñas: descubre cómo proteger más tu seguridad

Seguramente alguna vez hayas escuchado que, **para garantizar tu seguridad digital, es muy importante que las contraseñas de tus cuentas y perfiles sean distintas** y, además, resulten difíciles de adivinar para los y las ciberdelincuentes.

La razón es muy sencilla: si utilizas la misma clave en todas tus cuentas y la averiguan en una, la seguridad de todos tus perfiles se vería amenazada. No obstante, **recordar esta variedad de códigos de verificación** con sus caracteres especiales, números y combinaciones de letras **puede llegar a resultar complicado.** Es por eso que te recomendamos utilizar la herramienta del **gestor de contraseñas.**

Junta de Andalucía

Agencia Digital de Andalucía

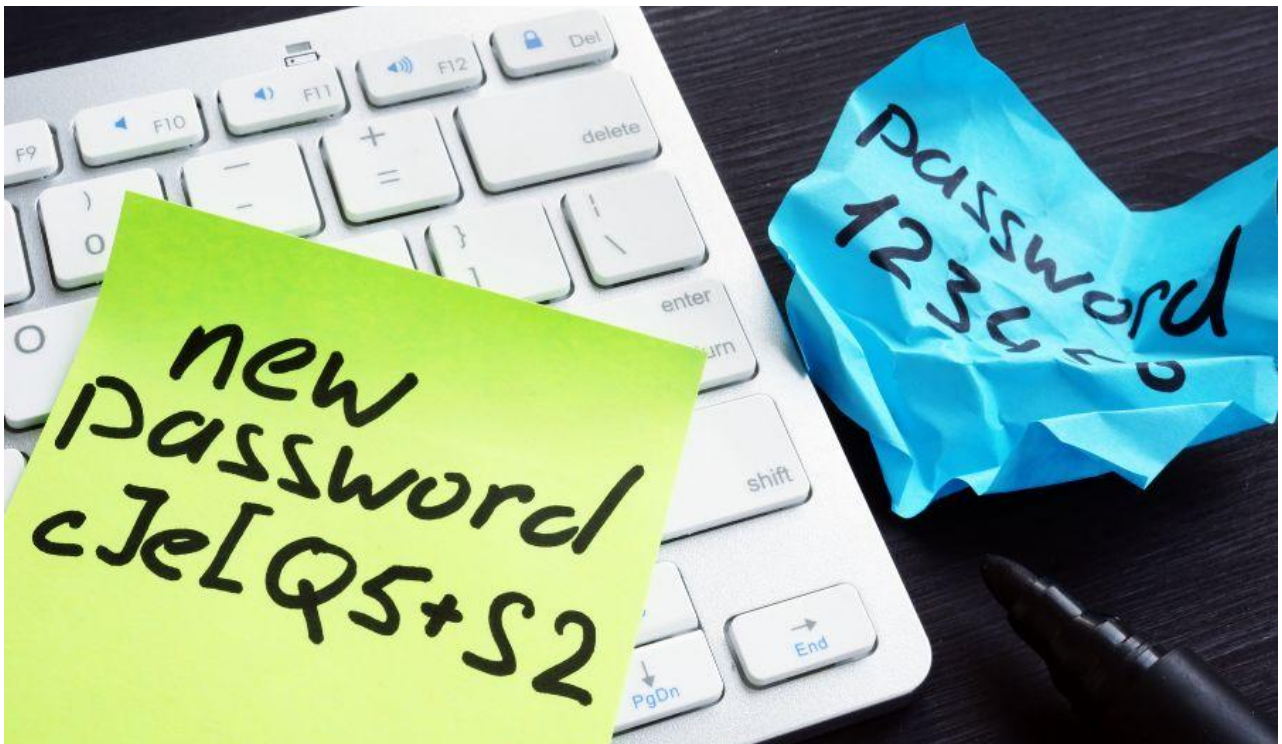
El método de apuntarlas todas a mano en una libreta a buen recaudo está bien, aunque con un gestor es mucho más sencillo, ya que te permite tenerlas todas a tu alcance en cualquier momento, sin necesidad de andar buscando entre papeles.

Pero, ¿son seguras estas herramientas? **¿Es fiable tener contraseñas almacenadas en el navegador?** La respuesta es clara: sí, siempre y cuando tomes ciertas medidas de seguridad.

¿Qué es y para qué sirve un gestor de contraseñas?

Cuando hablamos de un gestor de contraseñas, nos referimos a una **aplicación que nos permite guardar las distintas credenciales** y códigos de verificación que usamos para identificarnos en Internet. Es decir, no solo las almacena propiamente, sino que **las asocia con el correo electrónico** que hayamos seleccionado.

Podemos encontrar muchas aplicaciones muy sencillas de utilizar para llevar a cabo esta tarea. Todas se caracterizan por pedir una única **clave maestra**, mediante la cual se puede tener acceso al resto de claves almacenadas. Es fundamental que recuerdes esta contraseña principal, puesto que si la pierdes, no tendrás acceso al resto de credenciales que hayas guardado. No es una mala opción que la apuntes en una libreta o papel. En cualquier caso, **nunca la guardes en archivos de texto en tu ordenador o en notas del móvil**, puesto que si sufrieras un ciberataque, tu seguridad podría verse dañada.



Funciones que ofrecen los gestores

Como hemos señalado, hay distintas aplicaciones que ofrecen el **servicio de almacenamiento de contraseñas.** Dependiendo de la que elijas, las funciones que te ofrecen variarán, pero generalmente, estas herramientas incorporarán las siguientes:

- Podrás tener acceso a tus *passwords*, **aunque no tengas conexión a Internet**.
- Muchos gestores ofrecen la posibilidad de guardar todas las credenciales en un servidor externo a tu equipo, más conocido como **almacenamiento en la nube**. Suelen encontrarse cifrados, de tal manera que nuestros datos se mantienen protegidos. Esta opción es especialmente útil si vas a usar las cuentas en más de un dispositivo.
- Para aumentar la seguridad, algunas herramientas piden que se haga una **verificación en dos pasos**. Si tu teléfono móvil dispone de huella digital o te permite desbloquear el terminal con tu rostro, podrás seleccionar que además de emplear tu clave maestra te exija también un **factor biométrico**. Al tener esta doble seguridad, garantizarás que nadie, excepto tú, tenga acceso a esas contraseñas almacenadas.
- Normalmente, incorporan un sistema de **alertas de seguridad**. Cuando inicies sesión en un dispositivo que no es el habitual, te llegará un correo electrónico a tu cuenta principal para avisarte. Si alguien consigue acceder a tu cuenta, podrás estar sobre aviso y actuar en consecuencia.
- Si cuentas con un programa o extensión en tu navegador (*plugin*) para **autocompletar contraseñas**, estos gestores se conectarán a él. De esta manera, tendrás como automática la opción de que se complete la información. Para mayor seguridad, estas suelen pedir que se introduzca la **contraseña maestra**, o incluso la verificación en dos pasos.

¿Es seguro este gestor?

Es lógico que nos planteemos la seguridad de estas herramientas y que queramos saber que nuestras credenciales se encuentran a buen recaudo. Lo cierto es que **protegen de forma eficiente** la información que almacenan.

Las escasas **vulnerabilidades normalmente están asociadas a un comportamiento de riesgo** por parte de la persona usuaria. Por ejemplo, un error a evitar sería compartir el gestor de confianza con otros internautas o utilizar una clave maestra fácil de adivinar. En definitiva, recurrir a un gestor de contraseñas es mucho más fiable que anotar las claves en una libreta, o que usar la misma para todas las cuentas.

Gracias a la aparición de herramientas como estas podemos disfrutar de Internet con muchos menos riesgos, sabiendo que estamos protegidos mientras navegamos.

¿Cómo usar el gestor de contraseñas?

Para emplear alguno de estos gestores, lo primero es **descargar la aplicación**. Encontrarás aplicaciones diversas; busca la que mejor puntuación tenga en la plataforma en la que vayas a utilizarla. El punto positivo es que hay herramientas tanto para Windows como macOS, Android y demás sistemas operativos móviles. De esta forma, no encontrarás incompatibilidades. Estas son algunas recomendaciones que te hacemos: 1Password, LastPass, Dashlane, KeePass, Enpass, Keeper, Bitwarden, PasswordSafe y Roboform.

Una vez hayas descargado la aplicación seleccionada, tendrás que **crear una cuenta**. Recuerda: es fundamental que no olvides tu **contraseña maestra**. Será esta la que te abra el resto de puertas, y sin ella, no podrás acceder a tus contraseñas almacenadas.

Tras haberte identificado, encontrarás distintas maneras de utilizar la herramienta. En algunas aplicaciones tendrás que ir **introduciendo manualmente las cuentas** con los *passwords*, agregando los elementos uno a uno. No obstante, hay otras que te permiten **guardar esta información** conforme vayas accediendo a las redes sociales o las páginas webs correspondientes. Las ventajas del segundo método es que es más rápido, mientras que en el primero podrás añadir notas complementarias.

Combinando este gestor con la **opción de autocompletar disponible en los navegadores**, descubrirás una forma mucho más segura y efectiva de relacionarte con la tecnología. No tendrás que introducir constantemente datos difíciles de recordar, ni tendrás que recurrir a notas en el móvil, que son muy poco seguras.

Las contraseñas guardadas en Google: otro gestor

Si utilizas cualquier dispositivo que tenga asociado una cuenta de Google, ya llevas contigo un **gestor de contraseñas incorporado**. ¡Y muy fácil de usar!

En caso de que tengas un móvil Android, deberás **activar primero la herramienta**. Para ello, tendrás que ir a los ajustes del dispositivo, entrar en el apartado de '**Google**' y buscar la opción '**Autocompletar con Google**'. Cuando la habilites, recuerda entrar en '**Contraseñas**' si quieres ver todas las que ha ido almacenando tu cuenta.

Al estar incorporado en nuestros dispositivos, no tenemos que descargar una aplicación complementaria si no lo consideramos oportuno. No obstante, las funcionalidades que ofrece son más limitadas, con lo cual la elección de una herramienta u otra dependerá de tus necesidades.

Con Google podrás autocompletar los datos

Una vez lo hayas activado, podrás proceder a **autocompletar los campos**, como con cualquier otro gestor de códigos de verificación. Cuando vayas a introducir tu correo electrónico en cualquier página web, te aparecerá la opción de completar con una cuenta que ya tengas guardada, y no tendrás más que seleccionarla. A continuación, podrás elegir el *password* que también tenías almacenado. De esta manera, no tendrás que estar constantemente recordando datos.

Independientemente de que tengas un dispositivo que tenga Android o no, puedes usar estas contraseñas guardadas en Google siempre y cuando uses sus servicios. Por ejemplo, su navegador.

Prioriza tu seguridad: un generador de contraseñas seguras

Como habrás podido comprobar, las **ventajas** asociadas a un gestor de estas características son muchas. Podrás **cumplir con las pautas de seguridad** que recomiendan las personas expertas en este ámbito sin necesidad de estar apuntando cada código de verificación en un cuaderno. ¿Cuáles son estas pautas? Te las detallamos a continuación.

En primer lugar, lo recomendable es que tus contraseñas contengan **más de ocho caracteres** de longitud.

- No han de contener solo **mayúsculas** o solo **minúsculas**: lo ideal es combinar ambas.
- Además de letras, tiene que llevar un caracter o **símbolo** especial.
- Junto a esto, añadir al menos un **número**.

Es importante que la contraseña que elijamos sea **única** y, sobre todo, **no sea fácil de adivinar** por cualquiera que nos conozca. Nada de poner el nombre de nuestra mascota, nuestra fecha de cumpleaños o nuestra comida preferida. Un modo fácil de conseguir un código de acceso seguro sería pensar una frase que tenga cierto significado para ti. Por ejemplo, "En el pueblo de Jimena ponen croquetas a 3 euros". Ahora selecciona la primera letra de cada palabra y el resultado sería «EepdJpca3€».

Otra opción es recurrir a **un generador de contraseñas seguras** para garantizar que nuestros códigos de verificación cuentan con el nivel de seguridad necesario. Para esta tarea puedes consultar herramientas como Dashlane Generador de contraseñas, Perfect Passwords, Secure Password Generator y 1Password Strong Password Generator, entre otros.

Habrás observado que el mejor remedio para disfrutar de la tecnología con seguridad es aprender a **tomar las precauciones necesarias y contar con las herramientas adecuadas**. Como por ejemplo, un gestor de contraseñas que aporte una primera barrera de defensa frente a los riesgos de la red.

vuela

3.3

Copia de seguridad: protege todos tus archivos y datos personales

Imagina, por un momento, que toda **la información que tienes almacenada** en tu teléfono móvil o en tu ordenador **desaparece**. De la nada, sin previo aviso, y sin tener la posibilidad de acceder de nuevo a todos esos datos.

En ese momento seguramente te arrepientas profundamente de no haber hecho con antelación una **copia de seguridad o *backup***.

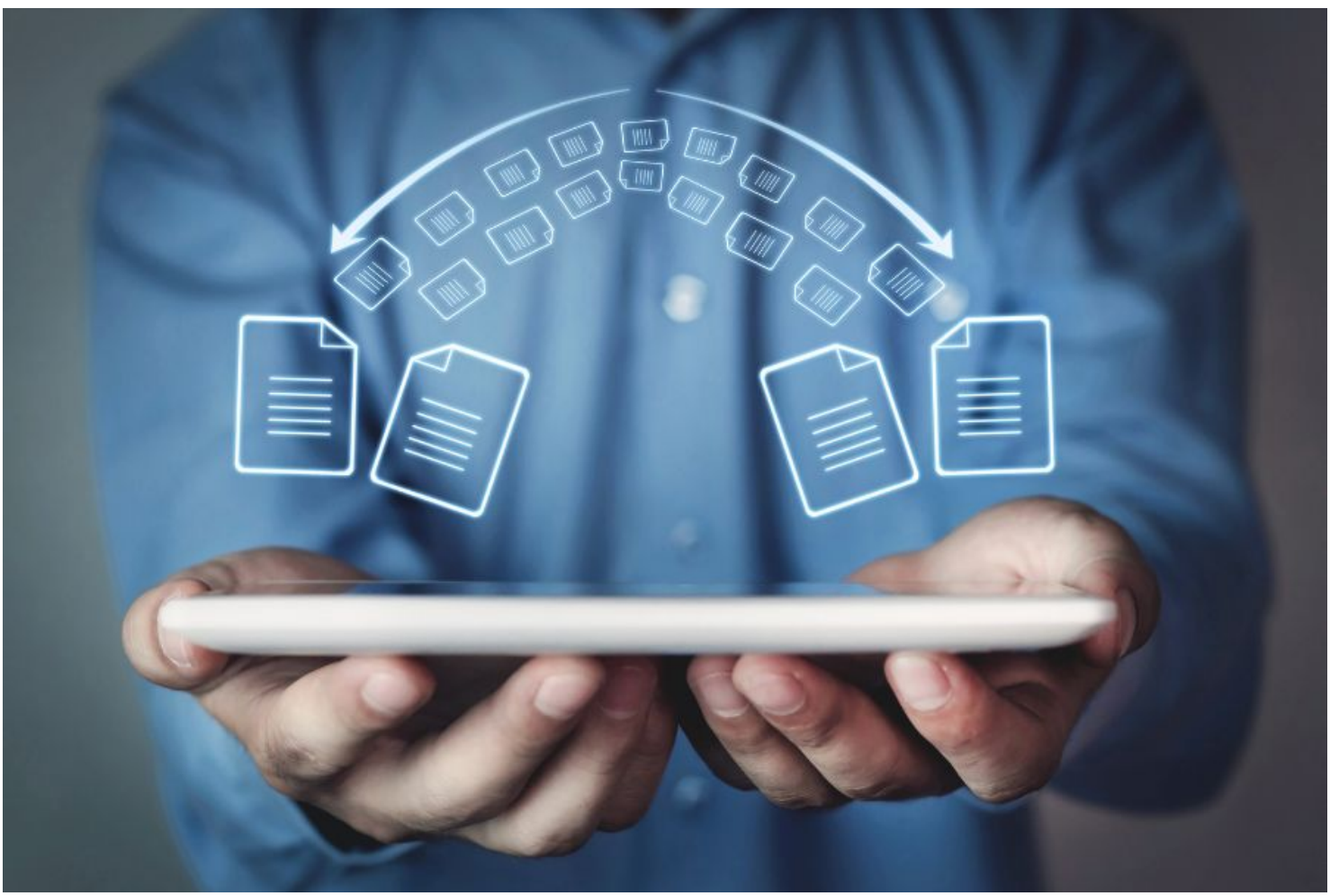
Junta de Andalucía

Agencia Digital de Andalucía

¿Por qué se puede producir una pérdida de información?, te estarás preguntando. Lo cierto es que las causas que lo originan son muy diversas: una rotura del disco duro, una aplicación que provoque el cierre inesperado del sistema o bien un *malware* o virus malicioso que afecte a tu ordenador, por citar algunos ejemplos.

Como ves, son muchos los factores que pueden desencadenar una pérdida de información. Por eso, lo mejor es anticiparse y **programar un *backup*** para que se realice regularmente en tus principales dispositivos.

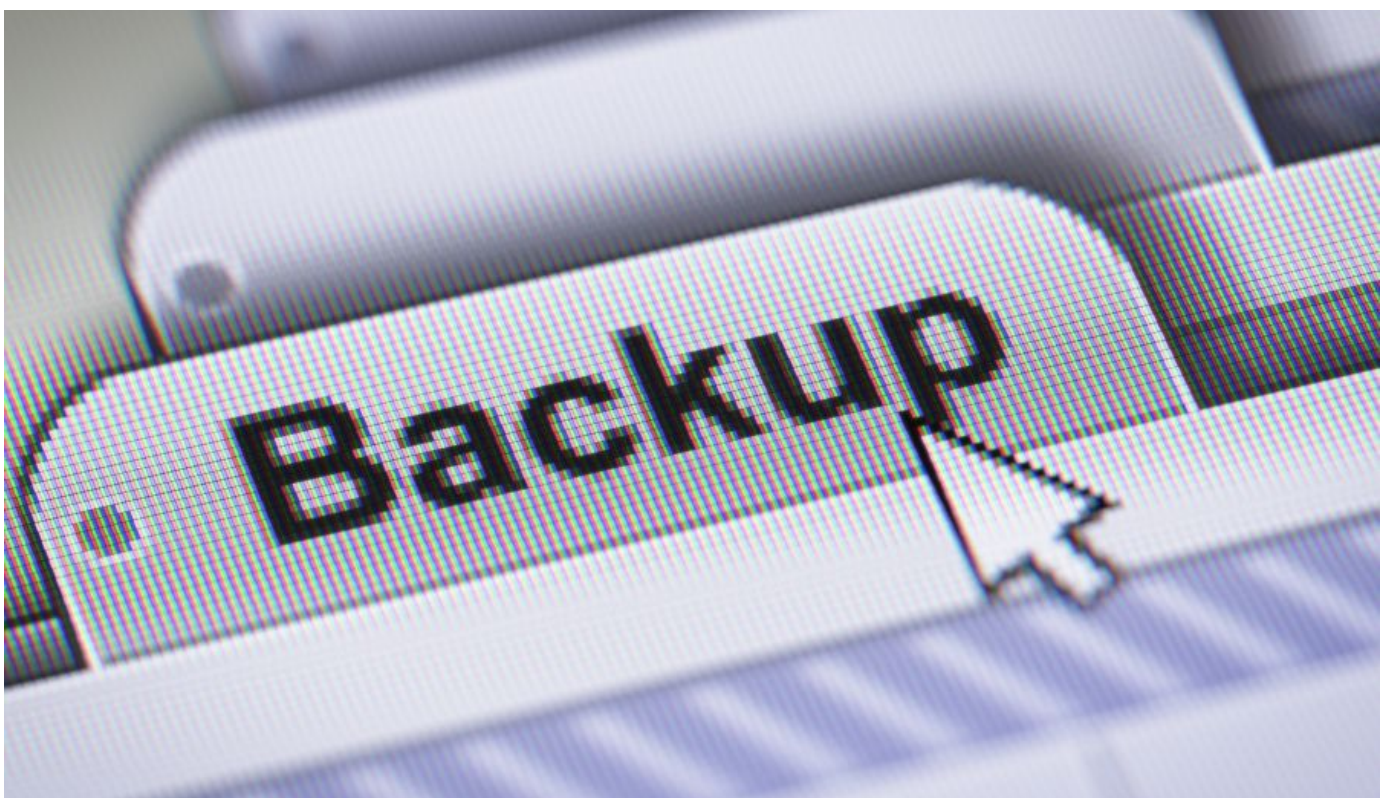
Mediante las copias de seguridad, tenemos la garantía de ir registrando **periódicamente** todos esos datos que no queremos perder bajo ningún concepto. Si no sabes exactamente a qué nos estamos refiriendo, continúa leyendo. ¡Te explicamos paso a paso qué es y cómo realizar una copia de seguridad para proteger tus archivos!



¿Qué es una copia de seguridad?

En primer lugar, aclaremos qué es una copia de seguridad. Básicamente, este procedimiento **consiste en hacer un duplicado de toda nuestra información personal**. Esta puede contener tanto documentos y archivos **que no queremos perder** como nuestros contactos, fotografías o incluso vídeos personales. A su vez, también es capaz de guardar los **perfiles, cuentas y certificados digitales** que dispongamos. En definitiva, esta herramienta de seguridad nos permite guardar una copia de todo aquello que hace de nuestro ordenador o nuestro teléfono móvil una herramienta de ocio o trabajo ideal. Las podemos hacer en dispositivos físicos, como **un disco duro externo**, o mediante un **servicio de almacenamiento en Internet**, más conocido como la nube.

Lo ideal es **programar** estos duplicados para que se hagan **automáticamente** y se almacenen en un aparato que no sea el que utilizamos habitualmente. Hay muchas aplicaciones que ofrecen este servicio, pero también los propios sistemas operativos incluyen la posibilidad de hacerlo. Si se opta por hacerlo de forma manual, sería conveniente que realices copias de seguridad semanalmente. No obstante, dependerá del valor de la información que contenga cada dispositivo y el riesgo que implique su pérdida.



Por ejemplo, si se trata de un ordenador de trabajo en el que se almacena toda la documentación, sería mejor no confiar en nuestra memoria para recordar que debemos realizar copias de seguridad con regularidad. Dejar que sea un **programa informático el que efectúe de forma automática y periódica los duplicados** será mucho más seguro. También encontrarás empresas que se dedican de manera profesional a almacenar los datos de sus usuarios. Es una buena opción en ciertas profesiones que requieren el uso de información importante diariamente.

Antes de crear una copia de seguridad, es interesante **analizar previamente qué es lo que necesita ser guardado**. Recuerda que **estos duplicados ocupan espacio** y no merece la pena almacenar datos erróneos o que ya se encuentran almacenados en otros dispositivos. Lo mejor es que antes de poner en marcha la copia de seguridad lleves a cabo una **limpieza de archivos innecesarios** o duplicados.

Mediante este método, preservarás todos los datos personales y archivos que usas en tu día a día, evitando así problemas posteriores.

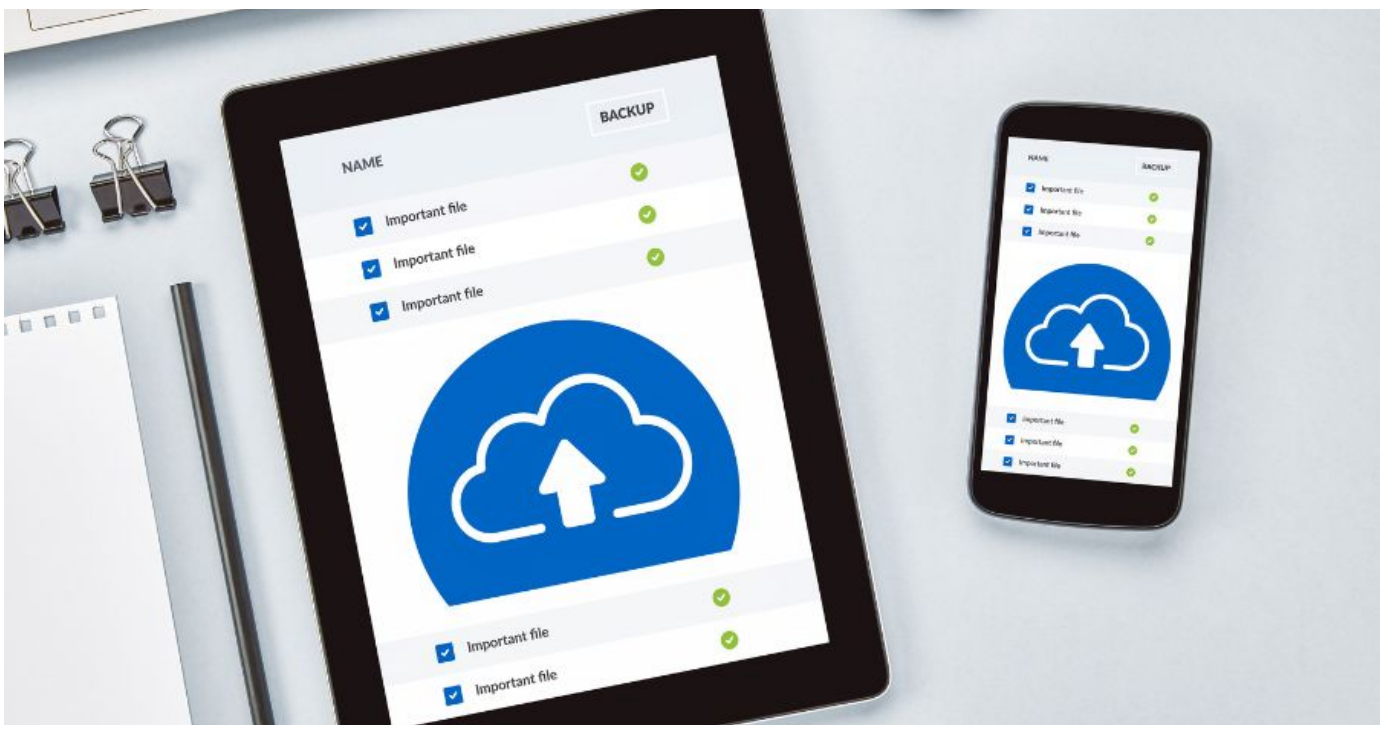
¿Cómo hacer un *backup* en los distintos dispositivos?

Una vez comprendido el concepto, pasemos a ver cómo podemos hacer una copia de seguridad en los distintos sistemas o aparatos. Para esto, necesitarás un dispositivo externo, como un **disco duro** o una **memoria USB** (*pendrive*), aunque también te explicaremos cómo hacer un ***backup* en la nube** por si te resultara más cómodo o no contaras con dispositivos externos.

Windows

Con Windows, el proceso es bastante sencillo. Vamos a explicar como realizar una copia de seguridad paso a paso en su versión 10, aunque en todas las versiones se realiza el mismo procedimiento:

- En primer lugar, tendrás que ir a '**Configuración**', y pulsar en **'Actuación y seguridad**'.
- Busca el apartado '**Copia de seguridad**'. Aquí tendrás la opción de '**Agregar una unidad'**, para añadir el dispositivo externo. Una vez pulses este botón, te aparecerán los que tienes conectados al ordenador.
- Cuando selecciones el dispositivo que consideres oportuno, señala que esta copia se haga en **modo automático**.
- Tras esto, podrás optar por obtenerla en ese momento para tenerla ya almacenada.



Android

No solo aconsejamos realizar **duplicados de seguridad** en los ordenadores. También es interesante hacerlos de manera periódica en los **móviles**, ya que es una herramienta que usamos diariamente para navegar por Internet, comunicarnos con otras personas y, en ocasiones, incluso para trabajar. De ahí la importancia de **salvaguardar la información** que contengan.

Para los teléfonos móviles con sistema operativo Android, lo más cómodo y rápido es optar por crear una **copia de seguridad en la nube** (suele venir instalada por defecto) y obviar los dispositivos externos. El almacenamiento en la nube siempre es mucho **más seguro**. Pero, recuerda, durante todo el proceso tendrás que **mantenerte conectado a la red** y lo que tendrás que hacer es:

1. Ir a la aplicación de **Ajustes** de tu teléfono.
2. Seleccionar el botón de '**Google**' y, dentro de este, '**Hacer copia de seguridad**'.
3. Una vez dentro, tendrás que darle al botón de '**Crear una copia de seguridad**'.

Una vez termine este proceso, ya tendrás todos tus datos guardados y podrás acceder a ellos mediante la aplicación de Google Drive. Este método es especialmente práctico **si cambias de teléfono** con frecuencia o si tienes pensado hacerlo en breve. Así **no perderás la información** y la configuración del nuevo dispositivo será mucho más cómoda.

iPhone e iPad

¿Y para los dispositivos de Apple? En este caso, existen dos formas de crear una copia de seguridad; podemos hacerlas o bien a través del Mac (el ordenador de esta marca), o bien a través de iCloud (similar a Google Drive). Esta última opción es la más recomendable si lo que tienes es un iPhone o un iPad. Para realizarlas, sigue estos pasos:

1. Ve a tu perfil dentro de la aplicación de '**Ajustes**', y pulsa '**iCloud**'.
2. Haz clic en el botón '**Copia de seguridad de iCloud**'.

Al igual que en Android, este proceso **requiere que estés conectado a Internet**. Se pueden **programar** y tu propio dispositivo te indicará cuándo fue la última vez que se hizo una copia de seguridad.

Ordenadores con mac iOS

En los ordenadores de Apple también puedes usar iCloud para almacenar todos tus archivos. Si quieres llevar a cabo un **duplicado del sistema completo**, podrás usar Time Machine, que ya viene integrado en su sistema. Para ello necesitarás, al igual que con Windows, **disponer de una unidad externa**. Tras conectarla, abre '**Time Machine'** en el menú, y busca dentro de sus preferencias la opción '**Seleccionar disco de copia de seguridad**'. Te aparecerán los que tienes disponibles para que selecciones la unidad externa de tu preferencia.

Para mayor protección, puedes seleccionar la pestaña en la que aparece '**Encriptar copia de seguridad**'. Con esta opción garantizarás que solo se pueda acceder a tus copias de seguridad **mediante una clave**. Tras esto, solo tendrás que efectuar la copia con normalidad. Recuerda que la primera vez siempre será más lenta que el resto, puesto que tienen que guardarse muchos más archivos y datos de sistema.

Linux

Si el sistema operativo que tienes en tu ordenador es Linux, puedes hacer un ***backup* parcial o integral.** En este caso, vamos a ver cómo hacer uno completo para proteger todos nuestros datos.

Lo más cómodo en este sistema operativo es optar por una **aplicación externa** que se encargue de hacer el trabajo, como es KBackup. Una vez la inicies, podrás observar en la parte izquierda una sección donde podrás **elegir los archivos que quieres proteger**. Solo tendrás que ir marcándolos; en un primer momento, es buena idea señalarlos todos.

A la derecha de la pantalla podrás elegir **en qué destino quieres guardar estos archivos**. Como en Windows o macOS, lo ideal es optar por una **memoria externa**. De esta forma, si se daña el ordenador, nos aseguraremos de tener en otro dispositivo nuestros datos.

Con esta aplicación también puedes crear **copias de respaldo automáticas**, con lo cual será mucho más sencillo asegurar que las realizas con la frecuencia adecuada.

La seguridad del almacenamiento en la nube

Hacer **duplicados en la nube** es invertir en tranquilidad. En la actualidad, muchas empresas se encargan de gestionar los *backups* de particulares o compañías. Contar con **servicios especializados**, llevados a cabo por equipos expertos, puede suponer un alivio en caso de ciberataque. Imagina perder todos los datos que tengas almacenados de la facturación de tu empresa, los contactos de tu teléfono móvil o los trabajos guardados de la universidad.

Si estás pensando en crear un respaldo de tus archivos, recuerda que es fundamental que hagas una **lista** de todo aquello que necesitas proteger. Es decir, qué **archivos, documentos o certificados** consideras **imprescindibles**. Tras esto, podrás decidir **cómo realizar ese duplicado**. Quizás ocupe muy poco espacio y puedas hacer tu mismo una copia de seguridad en la nube. Sin embargo, si lo que necesitas es protección para la información de tu negocio, ten presente que existe la posibilidad de contar con profesionales que te pueden asesorar.

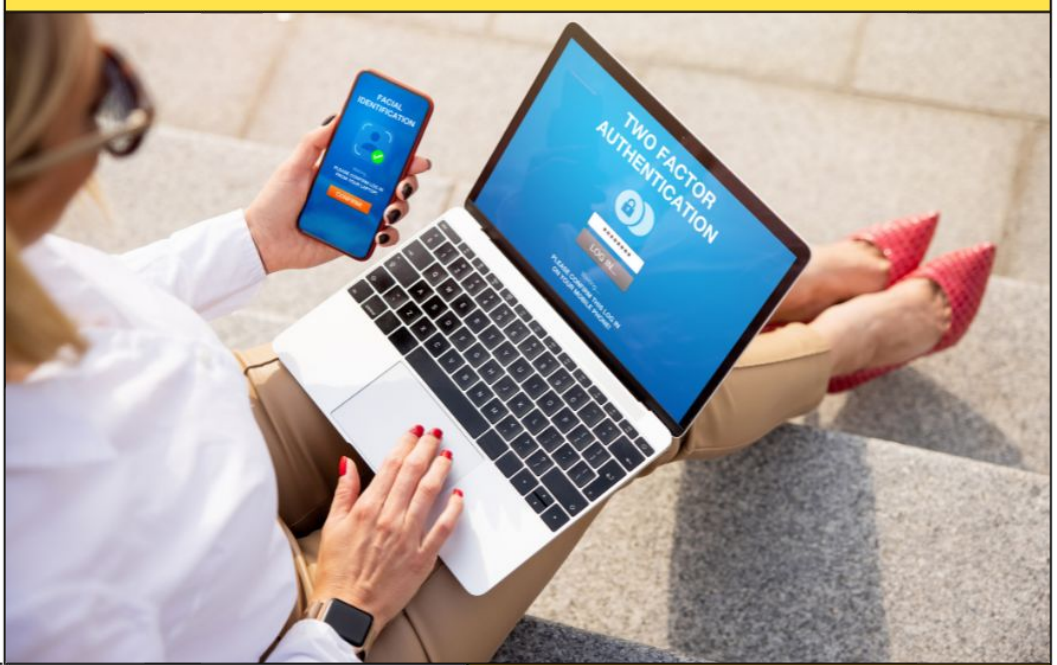
Las nuevas tecnologías traen consigo una multitud de oportunidades que puedes aprovechar. Estamos en la era de la información y la comunicación, y tenemos a nuestro alcance todo el conocimiento del mundo. No dudes en utilizar una **copia de seguridad** para tener la tranquilidad y la certeza que, ante cualquier imprevisto, tus archivos están resguardados.

vuela

3.4

¿Qué es la autenticación de doble factor y cómo puedes activarla?

Cuando interactuamos en redes sociales o a través de cualquier tipo de portal digital, no podemos bajar la guardia. Recuerda que, aunque el sitio web sea conocido para ti y cuente con las medidas de seguridad necesarias, hay ciberdelincuentes que utilizan estas plataformas para robar información o hacerse con el control de las cuentas. Para evitarlo, **la autenticación de doble factor (o autenticación en dos pasos) supone un nivel adicional de seguridad** a tu contraseña que deberías tener en cuenta. ¿Sabes cómo funciona y cómo activarla en tus dispositivos?

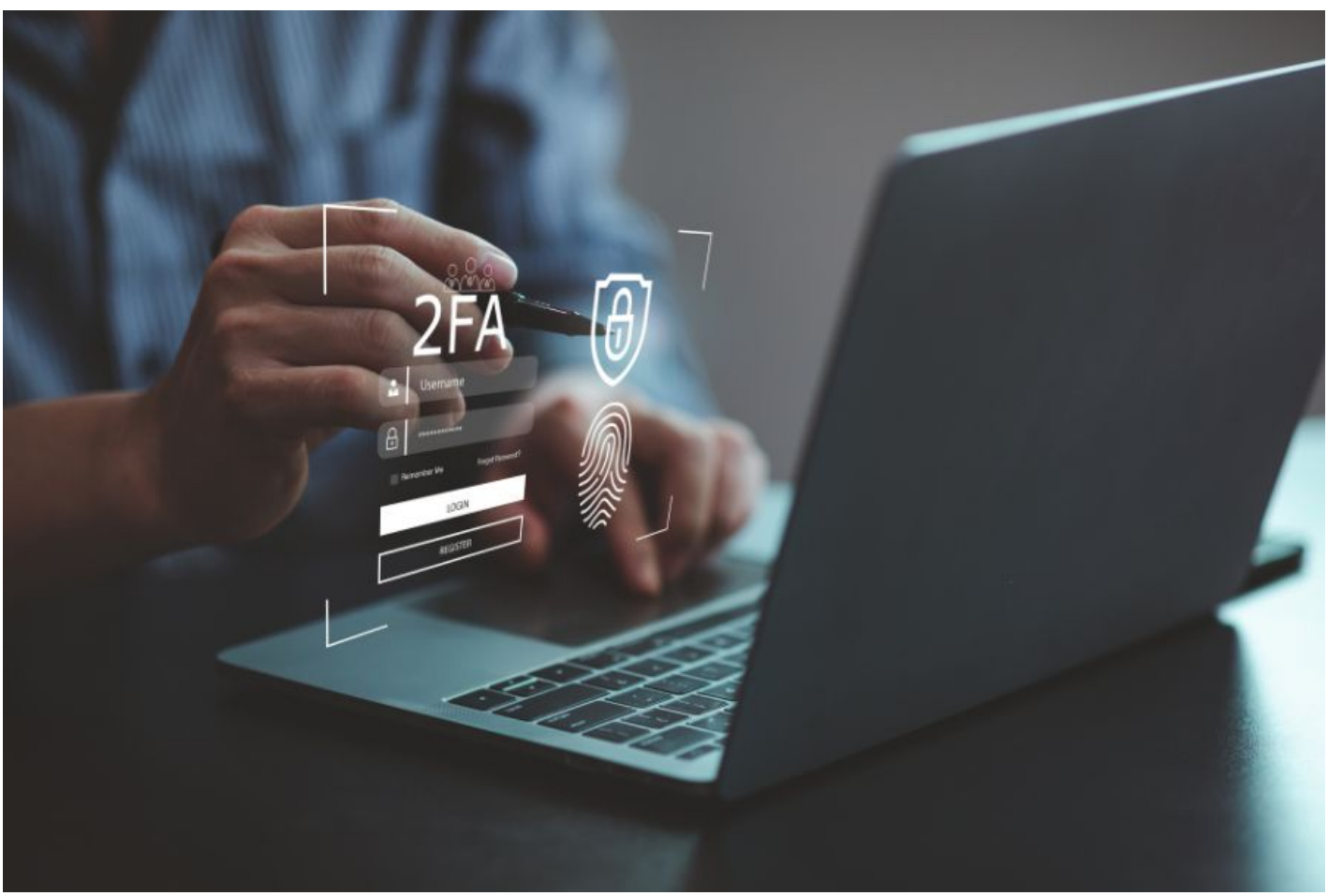


Junta de Andalucía
Agencia Digital de Andalucía

¿En qué consiste?

Si inicias sesión en tu cuenta dentro de una página web, necesitas proporcionar tu nombre o apodo y tu contraseña. Sin embargo, si un o una ciberdelincuente consigue averiguar tu clave tendrá acceso directo a tu cuenta. Por tanto, **es necesario que eleves un grado el nivel de protección, especialmente en aquellos espacios con información sensible**, como tus redes sociales, cuentas bancarias y portales de empresa. De este modo, **aunque tu contraseña se vea expuesta, tu información seguirá protegida**.

La autenticación en dos pasos (también denominada 2FA) implica **usar dos tipos de clave para acceder a tu cuenta.** En primer lugar, necesitas facilitar tu **contraseña** como es habitual. Una vez introducida la clave, el siguiente paso será conocer un **código recibido en tu móvil**, a menudo por SMS o enlace, que también deberás escribir en la página web para completar tu identificación y permitir el acceso.



Hoy en día, hay muchos sitios que ya emplean este sistema. Entre ellos, destacan varias plataformas conocidas, como Google y Twitter. Como ves, este sistema de acceso a tus perfiles apenas requiere unos segundos más y te permite evitar los ataques informáticos y los robos de información. Por tanto, es una técnica que deberías tener en cuenta.

Si bien la autenticación en dos pasos más popular está basada en la **segunda contraseña**, puedes encontrar otros sistemas:

- **Reconocimiento biométrico**: mediante la huella dactilar o el reconocimiento facial.
- **Autenticación física**: a través de una tarjeta de identidad (no el DNI) o similares.

¿Y la autenticación de múltiples factores?

En este caso, el **nivel de seguridad es mucho mayor**, puesto que necesitas aportar más de dos claves. De esta forma, las recibirás en tu correo o en una aplicación que tú conozcas. La primera ya la conoces, ya que se trata de tu contraseña normal. Las demás, por su parte, se generan aleatoriamente y cambian con cada inicio de sesión.

Al igual que en el caso anterior, **los medios más frecuentes para recibir los códigos son el correo electrónico o el SMS**. No obstante, **también puedes recibirlos a través de un certificado digital**. La Administración Pública, por ejemplo, ofrece este sistema de protección para realizar trámites a través del teléfono móvil o del ordenador.

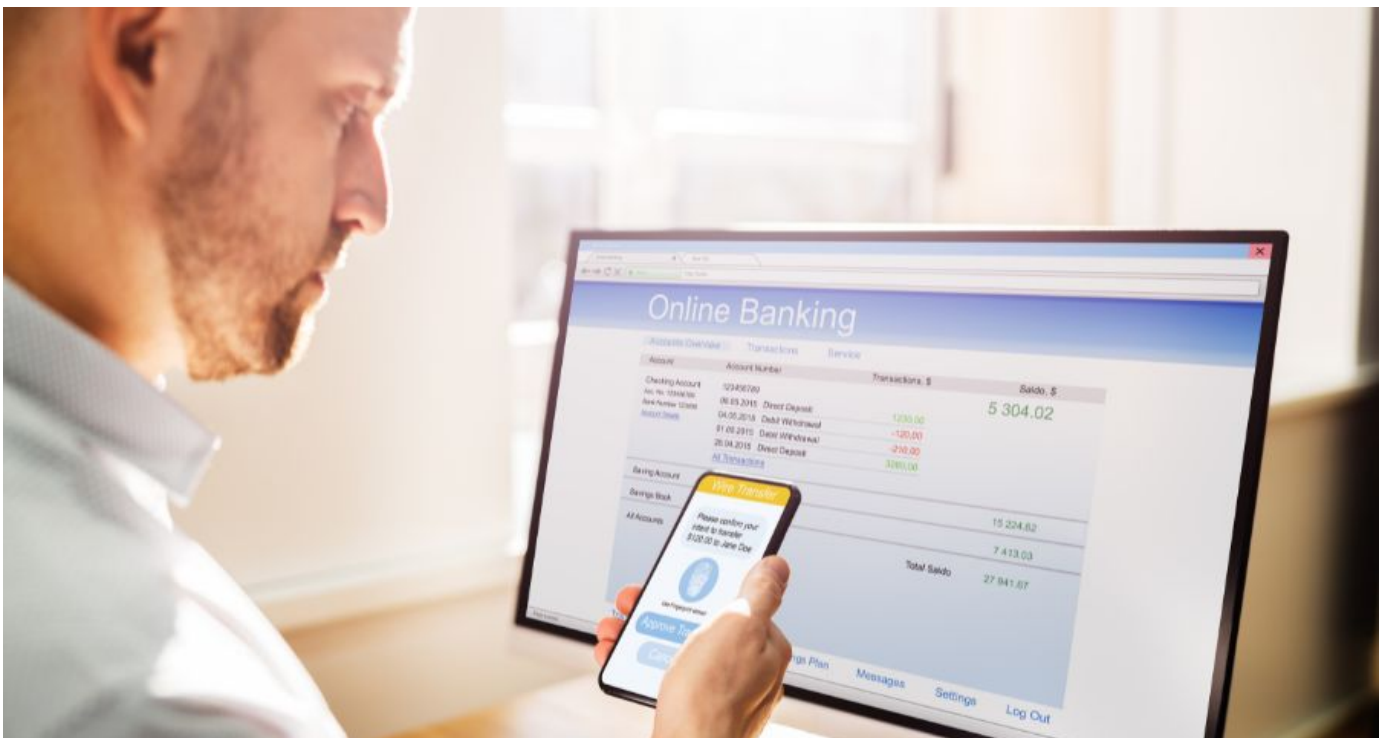
¿Dónde y cuándo necesito la autenticación múltiple?

La respuesta a esta pregunta dependerá de tu uso de Internet. En función del nivel de seguridad que necesitas garantizar, **podemos catalogar varios tipos de cuentas en la red**. Exponemos algunos ejemplos, ordenados de mayor a menor nivel de seguridad:

- Cuentas bancarias.
- Portal de la empresa.
- Aplicación de videoconferencia para clases *online*.
- Correo universitario / escolar.
- Correo electrónico.
- Tiendas *online*.
- Redes sociales.

Obviamente, **las cuentas bancarias requieren un nivel de seguridad bastante elevado**, pues son uno de los principales objetivos de ciberdelincuentes. Lo más normal es que la propia entidad te proporcione varios métodos de autenticación, así que solo tienes que activarlos (después veremos cómo).

El portal de la empresa y las cuentas académicas también requieren un nivel de ciberseguridad considerable, ya que suelen **comprometer información personal.** Del mismo modo, un error de ciberseguridad por nuestra parte en una de esas cuentas se traduciría en una pérdida de fiabilidad para la institución.



Las tiendas *online*, por su parte, no suelen contener información sensible. Eso sí, **es fundamental que no guardes los datos de tu tarjeta de crédito en la página**, ni siquiera si el portal te lo recomienda. Lo mejor es que los pongas cada vez que hagas una compra y selecciones «Nunca» cuando te pregunte si quieres almacenarlos.

Por último, es cierto que las redes sociales son uno de los objetivos más comunes de quienes delinquen en Internet. Sin embargo, estos suelen recurrir a otros medios para cometer sus actos, como es el *phishing* (robo de información privada mediante engaños). Lo ideal es que nunca guardes información personal en este tipo de portales.

Para ayudarte a decidir el nivel de seguridad que necesitas en cada caso, te mostraremos varias preguntas que puedes plantearte para saber si una cuenta —del tipo de que sea— requiere contraseña o autenticación de dos o múltiples factores:

- ¿Almacena información personal o no?
- ¿La empleas para intercambiar mensajes con otras personas?
- ¿Tienes fotos o vídeos tuyos o de tus seres queridos?
- ¿Guardas información relativa a tu situación económica?
- ¿Es indispensable para tu trabajo o estudios?

Si la información que almacenas es sensible, necesitarás recurrir a la 2FA. En cambio, si necesitas todavía más seguridad, **será mejor que optes por la autenticación de múltiples factores**.

¿Contra qué riesgos te protegen?

Cuando utilizamos Internet, estamos expuestos y expuestas a gran cantidad de riesgos que, por suerte, pueden ser prevenidos fácilmente. Si todos y todas hacemos un uso correcto de las plataformas *online* evitaremos numerosos peligros y conseguiremos que la ciberdelincuencia tenga cada vez menos sitio en el ciberespacio.

La autenticación de doble o múltiple factor te protege, entre otros, de los siguientes riesgos:

Robo de datos

Los y las cibercriminales pueden acceder a tus cuentas con el objetivo de **conseguir información sobre ti**. De esta forma, consiguen tu dirección, tus contraseñas de otras páginas y tus datos personales.

Difusión de información sensible

Si alguien con malas intenciones consigue entrar a tus redes sociales, tendrá acceso libre a tus imágenes y vídeos, estando en disposición de difundirlas sin tu consentimiento o copiarlas.

Pérdida de reputación

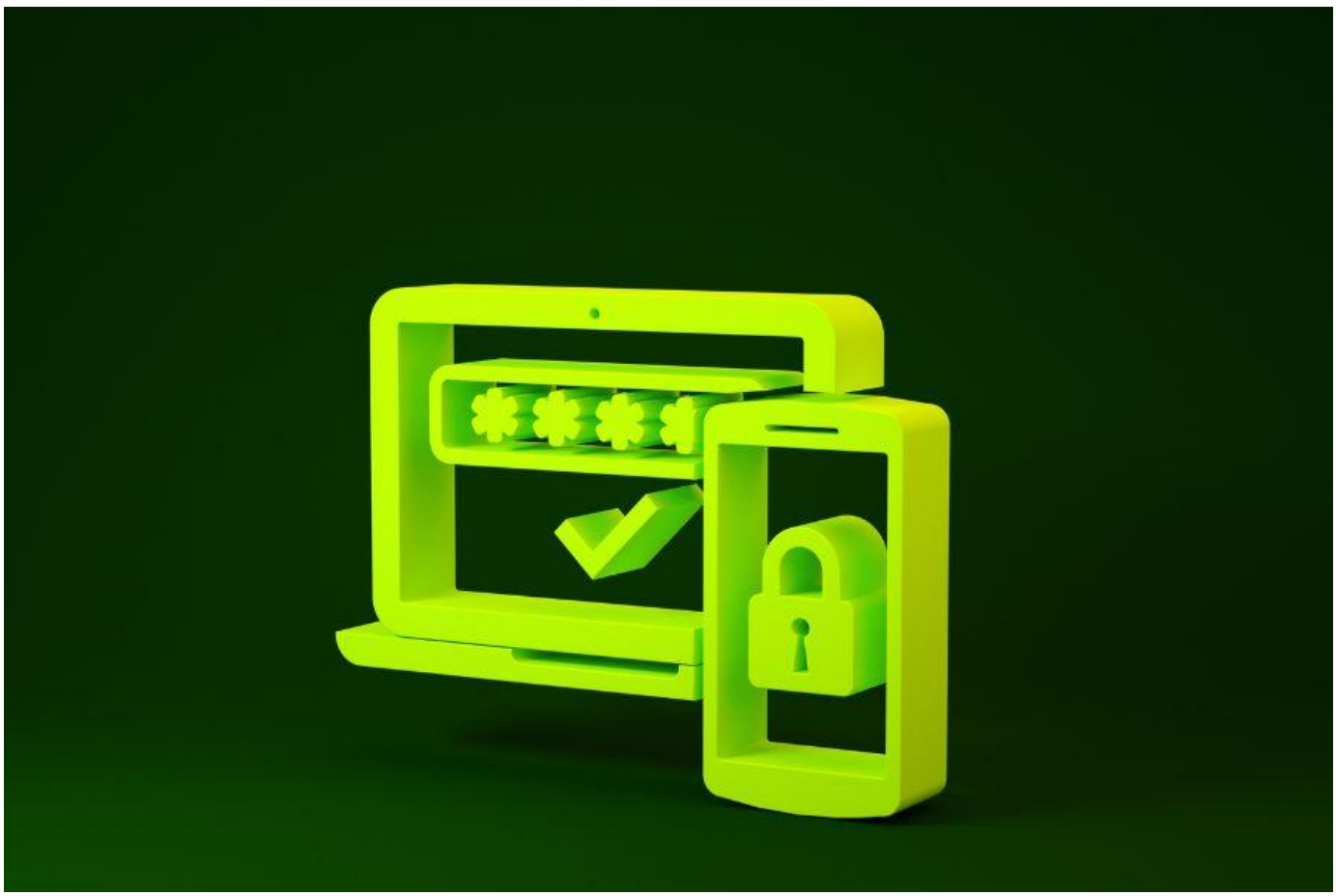
Si el robo se produce en la web de tu empresa, **puedes sufrir una pérdida de reputación**. Además, es posible que te consideren causante de un agujero de seguridad en la compañía.

Suplantación de identidad

A la hora de cometer delitos, las y los ciberdelincuentes nunca usan su verdadera identidad, sino que la suplantan. En este sentido, podrían hacer uso de tu nombre, apellidos y demás información para construirse un perfil falso.

Extorsión

Si acceden a tu información personal, **pueden utilizarla para conseguir dinero**. Muchos ciberataques se basan en el secuestro de datos y la petición de una recompensa para liberarlos (cosa que, por otra parte, no se suele producir).



¿Cómo proteger tus dispositivos?

Como has podido ver, proteger tus dispositivos es la mejor forma de evitar los riesgos que se asocian a ciberataques. Esta es una tarea que nos corresponde como internautas, por lo que es esencial que sepas cómo hacerlo. Según el dispositivo o el portal que emplees, tendrás que seguir un método u otro.

Google (Android y Gmail)

El correo de Gmail te permite realizar varios métodos de autenticación en dos pasos. Lo más común es que te envíe un **mensaje de texto con las claves de verificación** y, posteriormente, **recibirás una notificación en el móvil** para confirmar que eres tú quien va a acceder a la cuenta.

En tres pasos, tendrás esta modalidad activada:

1. Dirígete a tu cuenta de Google.
2. Accede al panel de navegación y después a «Seguridad».
3. Busca «Iniciar sesión en Google» y luego «Verificación en dos pasos».

Microsoft (Outlook)

En Outlook también tienes la posibilidad de activar la autenticación en dos pasos. Cada vez que inicies sesión (*login*) en un dispositivo que no has incluido en la lista de confianza recibirás también un **código de verificación que deberás introducir para acceder a tu *email***.

Para activar esta opción sigue los siguientes pasos:

1. Accede a tu cuenta de Microsoft.
2. Selecciona «Configuración de seguridad».
3. Elige «Verificación en dos pasos» > «Configurar la verificación en dos pasos».

Dispositivos de Apple

En el caso de los dispositivos iPhone, iPad y iPad Touch, la autenticación en dos pasos de iOS es bastante sencilla de comprender. Primero, tienes que proporcionar tu **contraseña normal**. Después, recibirás una **clave de seis dígitos** llamada «código de verificación» en un dispositivo que hayas seleccionado como de confianza o mediante SMS.

Para activarla, debes seguir las siguientes rutas:

1. Ajustes > [Nombre de usuario] > Contraseña y seguridad.
2. Pulsa en «autenticación de doble factor».

Si tienes un ordenador de iOS (Mac), también puedes activar esta capa de seguridad adicional. En este caso, selecciona igualmente un número de teléfono o un dispositivo de confianza en el que recibirás el código de verificación. **Este cambiará cada vez que cierres sesión**.

La activación requiere de tres pasos:

1. Accede al menú de Apple > «Preferencias del sistema» > «ID de Apple».
2. Ve a «Contraseñas y seguridad» (lado izquierdo).
3. Pulsa en «autenticación de doble factor».

Redes sociales

Veamos cómo puedes activar la autenticación múltiple en las redes sociales más utilizadas:

En **Facebook**, tienes que realizar la siguiente ruta:

1. «Configuración de seguridad e inicio de sesión».
2. «Usar la autenticación en dos pasos» > «Editar».
3. Escoge el método de seguridad (*app* de terceros, SMS o dispositivo compatible).

Para **Instagram**, debes seguir estos pasos:

1. Ve a tus ajustes y después a «Seguridad».
2. Selecciona «Autenticación en dos pasos».
3. Elige entre las opciones de seguridad a tu disposición.

Por último, esta es la ruta necesaria para **Twitter**:

1. Dirígete a «Más» > «Configuración y privacidad».
2. Escoge «Seguridad y acceso a la cuenta» > «Seguridad» > «Autenticación en dos factores».
3. Selecciona uno de los métodos que aparecen.

Como has visto, **la autenticación de doble factor es imprescindible** para aumentar la seguridad mientras usas Internet.

vuela

3.5

¿Para qué me sirve el bloqueo remoto y cómo hago para activarlo?

En la actualidad, los dispositivos inteligentes forman una parte fundamental de nuestra vida cotidiana, familiar y profesional. Los *smartphones*, *tablets* y ordenadores son un claro ejemplo de ello. Sin embargo, este nuevo entorno también tiene sus riesgos.

Por ello, es importante tener en cuenta funcionalidades como **el cifrado y el bloqueo remoto**. ¿En qué consisten y cómo te pueden ayudar a tener mayor seguridad?

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es el bloqueo o cifrado remoto?

Los móviles contienen numerosa información de valor, eso está claro. Seguro que almacenas gran cantidad de imágenes, vídeos, música, notas de recordatorio y contactos, por no hablar de los mensajes que intercambias con otras personas o tus cuentas en redes sociales. En definitiva, información que no debe caer en manos de terceros.

El bloqueo o el cifrado en remoto son indispensables para la ciberseguridad. Se trata de **funciones que los teléfonos incorporan para desactivarse automáticamente cuando reciben la orden de hacerlo**. Para ello, deben recibir la señal de su propietario o propietaria, generalmente, desde otro dispositivo de confianza.

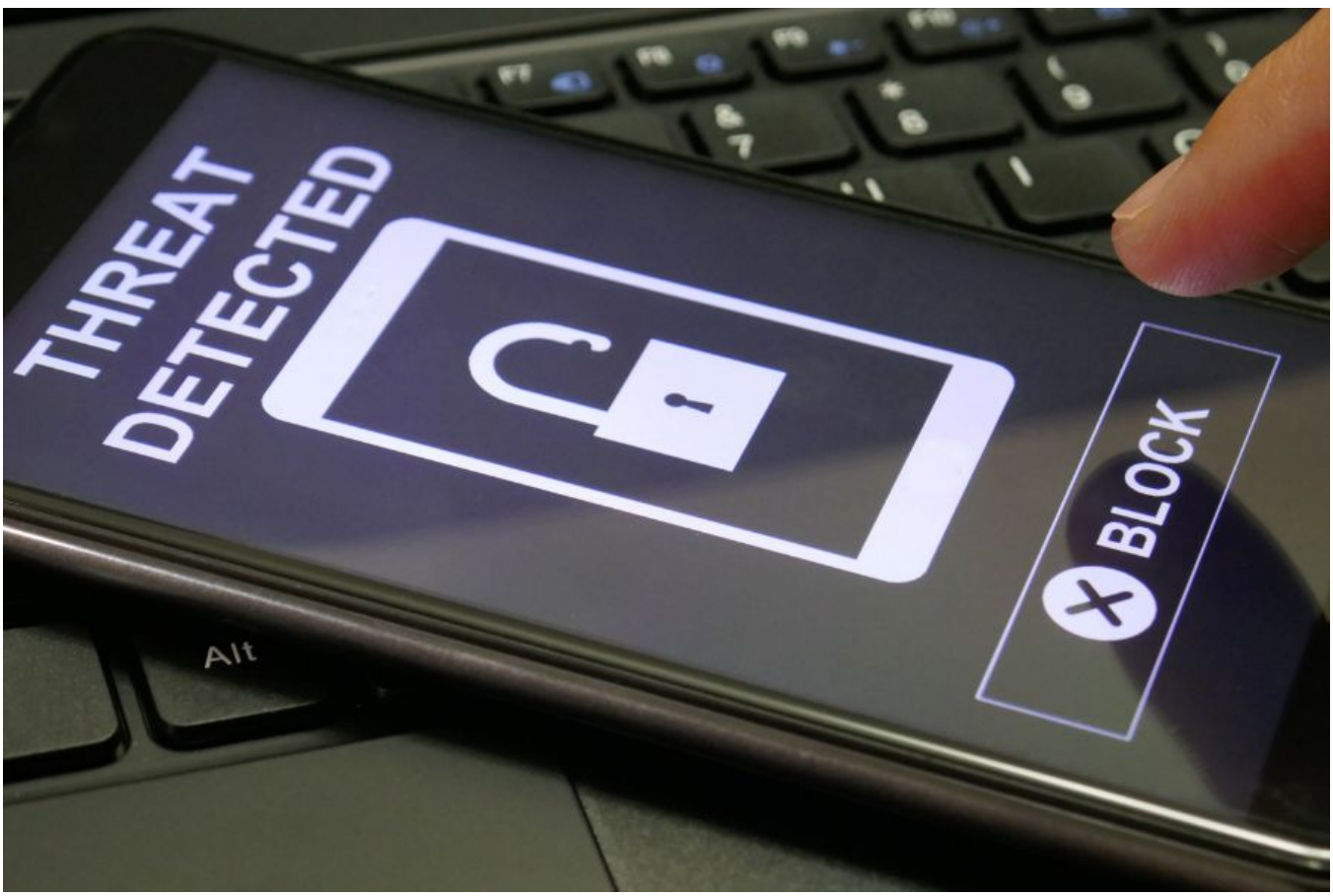
Con el término «cifrado», nos referimos a algo que seguramente ya habrás hecho tú: poner contraseña. De este modo, **tu teléfono deja de funcionar temporalmente** hasta que se escriba una combinación de letras, números o caracteres especiales que tú has escogido previamente. Claro está que lo mejor es elegir una **clave extensa y difícil de averiguar.**

Ambas funciones han ganado bastante difusión con el auge de la conectividad entre *smartphones*. También están disponibles en *tablets*, ordenadores y otros aparatos. **Incluso en los casos en los que los dispositivos no la incluyen de fábrica, es posible incorporarla** (después veremos de qué manera).

Para habilitar el bloqueo del teléfono a distancia, solo necesitas haber escogido previamente otro dispositivo de confianza. A través de este último, introducirás una clave que te identifique como el propietario o propietaria del *smartphone* robado o extraviado. Después, podrás activar su bloqueo para que nadie pueda acceder a tu información.

¿Cuándo necesitas recurrir al bloqueo remoto?

Como ya te podrás imaginar, hay dos circunstancias en las que deberás suspender tu teléfono a distancia: **si lo has perdido o si te lo han robado.** Independientemente del caso, **lo más importante es que lo hagas al poco tiempo de que haya sucedido**, ya que evitarás que otras personas tengan acceso a tu información privada.



¿Cómo activar el bloqueo remoto?

Lo más normal es que tu móvil tenga una función preinstalada de bloqueo remoto, independientemente de si es Android o iOS. Sin embargo, en ambos casos deberás habilitarla para que pueda funcionar. Obviamente, **requiere tu autorización al tratarse de un uso del GPS constante**.

Para **activarla en Android**, debes hacer lo siguiente:

1. Entra en ajustes y después en «Ajustes de Google».
2. Ve a «Seguridad» y elige «Encontrar mi dispositivo».
3. Habilita la opción «Permitir borrado y bloqueo remotos».

Tras esto, debes ir a los ajustes, volver a «Seguridad» y acceder a «Administradores de dispositivos». Si todo es correcto, te aparecerá que has puesto en funcionamiento la opción de encontrar tu móvil.

Si tu teléfono es de iOS, necesitas seguir estos pasos:

1. Dirígete a la aplicación Buscar y accede a «Dispositivos y objetos».
2. Escoge tu teléfono en la lista.
3. Selecciona la opción «Marcar como perdido» y ve a «Activar».

De esta manera, tu móvil quedará bloqueado en remoto. Además, **puedes configurar un mensaje que aparezca en la pantalla** para que la persona que lo tenga sepa a qué número debe llamar para avisarte.

¿Qué otras opciones tienes?

Si has perdido tu teléfono o te lo han robado, además de bloquear el dispositivo, también puedes llevar a cabo otras acciones. La principal es **denunciar**, ya que las autoridades podrán hacer las investigaciones correspondientes para dar con tu dispositivo. Para ello, **es fundamental que conozcas el IMEI de tu dispositivo** (el identificador exclusivo de tu teléfono móvil a nivel mundial). Tienes la posibilidad de hacerlo de las siguientes formas:

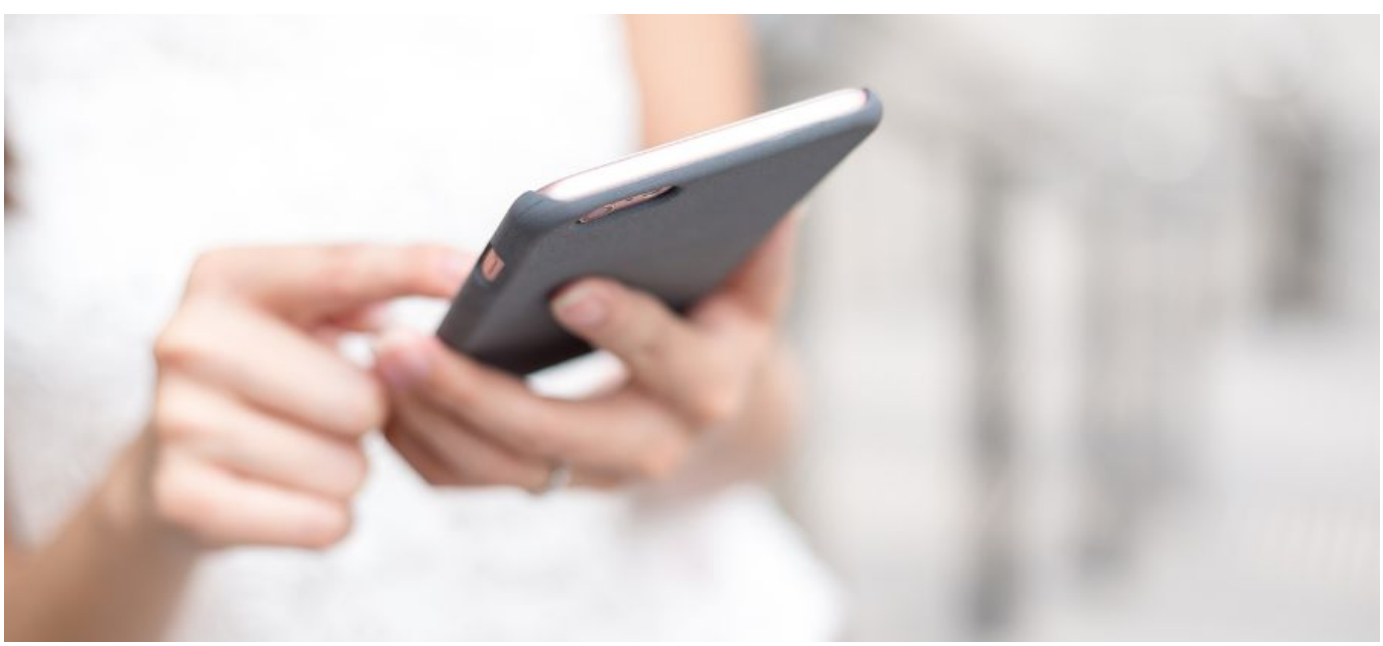
Método 1:

1. Accede a la aplicación de Teléfono.
2. Introduce lo siguiente: ***#06#**.
3. Aparecerá un mensaje con la denominación «IMEI» y un código de 15 dígitos.

Método 2:

1. Dirígete a los ajustes del móvil.
2. Entra en «Acerca del teléfono» > «Estado» > «Información de IMEI».
3. Dependiendo del modelo, te aparecerá en las primeras opciones.

Aunque con ligeros cambios, estos dos métodos te servirán para encontrar este código en terminales de todas las marcas, tanto de Android como de Apple.



Geolocalización

El **principal modo de encontrar tu móvil** es a través de la geolocalización. Esta, sin embargo, **tiene que haber estado activada antes** de que lo perdieras o de que te lo robaran.

Cómo activarla en Android:

1. Entra a los ajustes y después a opciones como «Datos biométricos» o «Seguridad».
2. Activa la opción «Encontrar mi móvil».
3. Habilita también las funciones **«Desbloqueo remoto» y «Enviar mi última ubicación».**

Así, tu teléfono enviará su localización cada 15 minutos, lo que te permitirá acceder a esta desde otro dispositivo y, lo más importante, quien lo tenga no podrá desactivarla si no conoce la contraseña.

Cómo activarla en iOS:

1. Ve a los ajustes y después a tu nombre.
2. Escoge «Encontrar» y «Compartir mi ubicación».
3. Activa la opción **«Buscar mi dispositivo»**.

Tras esto, deberás **habilitar la localización en tiempo real**. De este modo, un mapa te mostrará dónde está tu teléfono.

1. Dirígete a los ajustes y luego a «Privacidad».
2. Marca la casilla «Localización».

Gracias a esto, sabrás dónde está tu iPhone o iPad, **incluso si no tiene conexión**. Puedes también agregar otros productos de la misma marca, como los AirPods o el Apple Watch.

Encriptar el dispositivo

Esta opción lleva algo más de tiempo, pero es idónea si quieres aumentar todavía más la seguridad. **Encriptar es un paso añadido al simple bloqueo y consiste en añadir algún tipo de clave o sistema que impida el acceso a la información a las personas no autorizadas**. Para ello, **se recurre a medios biométricos** que son muy difíciles de suplantar, por lo que nadie más que tú tendrá acceso a tu información. Estos medios que te mencionamos son:

- **Huella dactilar.** Es la más complicada de falsificar, ya que no hay dos iguales en el planeta.
- **Reconocimiento facial**. Es bastante útil, pero se puede desactivar con una foto nuestra en algunos modelos.
- **Escáner del iris**. Algunos teléfonos de última generación analizan nuestro iris mediante la cámara frontal.

Sea cual sea, lo mejor es que lo tengas también **protegido con contraseña o patrón** (mejor la primera). Así, blindarás el acceso a tu información personal y te protegerás frente a ciberdelincuentes.

Proteger las *apps* sensibles

Si alguien ha entrado a tu teléfono, tienes la opción de evitar que entre en las aplicaciones más sensibles y blindar, por ejemplo, tu galería de imágenes, lista de contactos o redes sociales. De este modo, no conocerá tu información personal y tu privacidad se verá menos comprometida.

Algunos modelos de teléfono incluyen la opción de bloquear determinadas *apps* de tu elección, sobre todo los más recientes. Sin embargo, otros no la tienen instalada de fábrica. Ante esta situación, **descárgate un *software* (*app*) de Internet que lleve a cabo esa tarea**: AppLock – Huella Digital, CM Security AppLock Antivirus o Smart AppLock son algunas alternativas. Todo depende del *smartphone* que utilices y de tus necesidades.

Borrar por completo la información

Esta es la solución más extrema, pero te puede ser de ayuda. **Si la información que tienes almacenada es demasiado sensible o tienes constancia de que no vas a recuperar el teléfono**, es mejor que lo formatees. Para hacerlo, debes realizar los siguientes pasos:

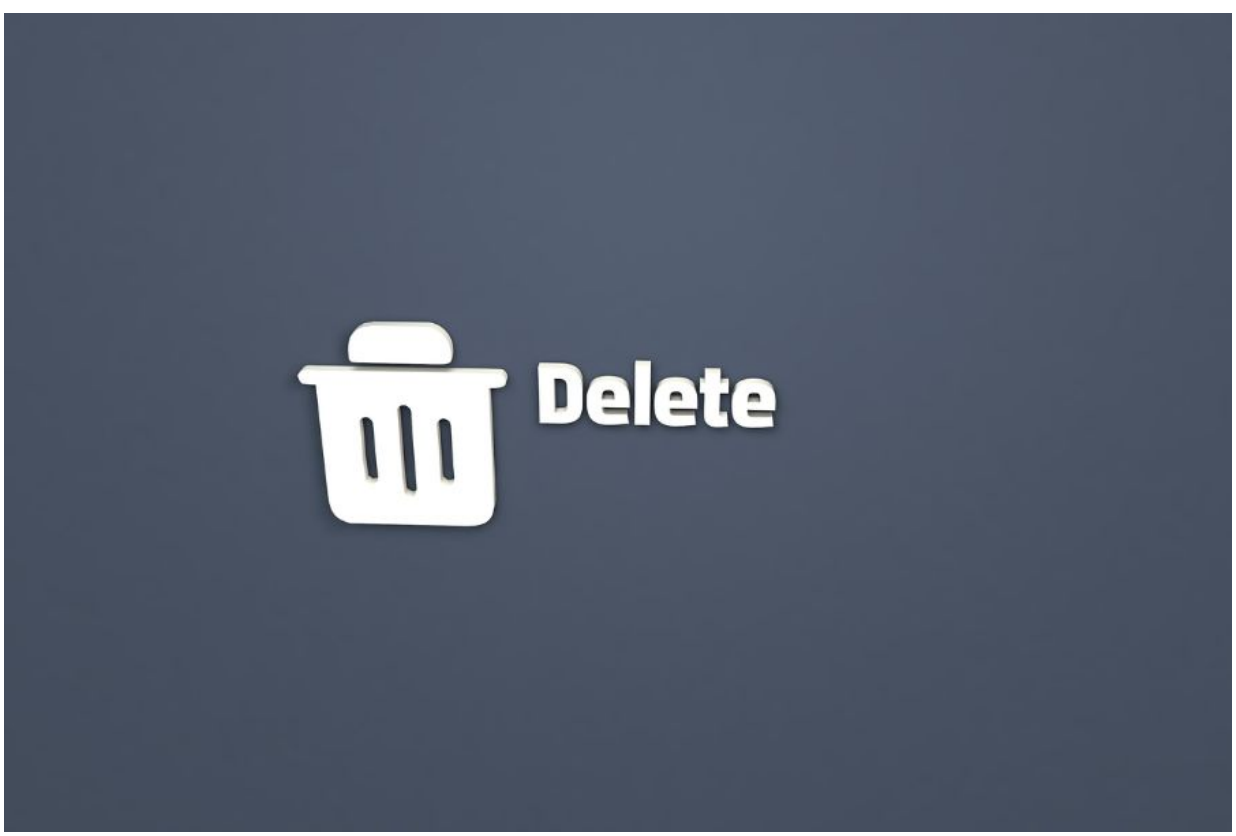
En Android:

1. Accede a los ajustes y posteriormente a «Seguridad».
2. Ve a «Encontrar mi dispositivo» y activa «Permitir borrado y bloqueo remotos».

En iOS:

1. Ve a los ajustes y pulsa en «Encontrar».
2. Activa «Buscar mi dispositivo».

Debes tener en cuenta que, si haces el borrado completo de los datos, tampoco podrás localizar en tiempo real el móvil.



¿Y en ordenadores? ¿Cómo protegerlos?

Tanto si tienes un portátil con sistema operativo Windows como si es un Mac, también puedes bloquearlos en remoto.

Windows

En primer lugar, **debes iniciar sesión como administrador** (es decir, con la cuenta principal de tu ordenador, si es que existen varias). Esto te otorgará los permisos especiales que necesitas. Ten en cuenta que no funciona si accedes con una cuenta local, aunque sea con privilegios de administrador.

Después, realiza la siguiente ruta: «Configuración» > «Actualización y seguridad» > «Buscar mi dispositivo» > «Activar ubicación» > «Cambiar» > «Guardar la ubicación de mi dispositivo periódicamente». De este modo, **tendrás tu disco duro encriptado**.

Mac

Al igual que en iPhone e iPad, el bloqueo a distancia se denomina «bloqueo de activación». Ten siempre en mente tanto tu contraseña como tu ID de Apple. Gracias a esta funcionalidad, nadie podrá entrar a tu ordenador, utilizarlo para ningún fin ni borrar su información.

Esta ruta te permitirá habilitarlo: «Menú Apple» > «Preferencias del sistema» > «ID de Apple» > «iCloud» > «Buscar mi Mac».Como has podido ver, el **bloqueo remoto** es esencial para garantizar tu seguridad cuando usas la tecnología. Lo más importante es que lo actives cuanto antes y que utilices algún medio de los que te hemos propuesto para localizarlo.

vuela

3.6

¿Qué son las herramientas de control parental? Guía para familias

Las **tecnologías digitales son una parte fundamental en la** **educación** de niños y niñas. El uso de dispositivos tecnológicos o el acceso a recursos formativos a través de Internet desde una edad temprana es una realidad **cada vez más presente** en los centros de enseñanza y hogares andaluces.

Por ello, es importante que desde la infancia aprendan a hacer **uso de las tecnologías de forma responsable**, evitando que puedan sentir miedo y permitiéndoles disfrutar de todas las posibilidades del mundo digital. Además, las familias tienen a su disposición útiles herramientas para **garantizar la seguridad** de sus hijos e hijas en la red. Por ejemplo, las **herramientas de control parental.**

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es el control parental?

Como bien sabes, la mejor forma de garantizar que tus hijos e hijas hagan un uso responsable de la tecnología empieza educando en seguridad digital desde la infancia, acompañándolos en el uso de dispositivos inteligentes y participando activamente en su vida digital.

No obstante, para reforzar su seguridad en la red podemos recurrir a las herramientas de control parental. Estas aplicaciones están diseñadas para complementar la supervisión que padres y madres realizan de la actividad de los menores en Internet y presentan numerosas ventajas, desde la opción de **filtrar los contenidos inadecuados** hasta la **limitación del tiempo de uso** de los dispositivos.

A través de este sistema de cuidados, **garantizarás un entorno *online* más seguro**. Lo mejor es que no ejerces la supervisión directa, que puede resultar más invasiva, aunque sí proteges su actividad ante posibles riesgos.

Frecuentemente, este tipo de herramienta está disponible **en todos los aparatos con conexión a Internet**. Las encontrarás en teléfonos móviles de cualquier marca, *tablets* y ordenadores, así como en las Smart TV o incluso en las consolas de videojuegos.

¿Cómo puedo instalar herramientas de control parental?

El sistema que acabamos de explicar es bastante versátil, ya que está presente en numerosos dispositivos de diferentes maneras. Así, **lo más frecuente es que se encuentre en una aplicación** que puedes descargar en teléfonos y *tablets*. En los ordenadores, por su parte, lo obtienes en programas que se adquieren en Internet. Más adelante te mostraremos en detalle algunas de estas opciones.

Otros aparatos, como las videoconsolas, lo incluyen de manera predeterminada en sus ajustes. Esto también se cumple en los teléfonos móviles diseñados para niños/as o en muchos de los teléfonos convencionales. Sea cual sea el caso, tienes la posibilidad de activar el control parental desde los ajustes, generalmente en las funciones de privacidad o seguridad (depende de la marca y del modelo).

Muchas de estas herramientas funcionan sin que la persona que está usando el dispositivo tenga conocimiento de ello. Sin embargo, **ten en cuenta que la base de la confianza es la comunicación**. Por tanto, lo más recomendable es que tus hijos o hijas sepan que su uso de Internet será supervisado por su seguridad. De este modo, aprenderán a utilizarlas de forma responsable.

¿Cómo te ayudan las herramientas de control parental?

Todo depende del dispositivo, pero lo más común es que incluyan las siguientes funciones.

Restringir el contenido inapropiado

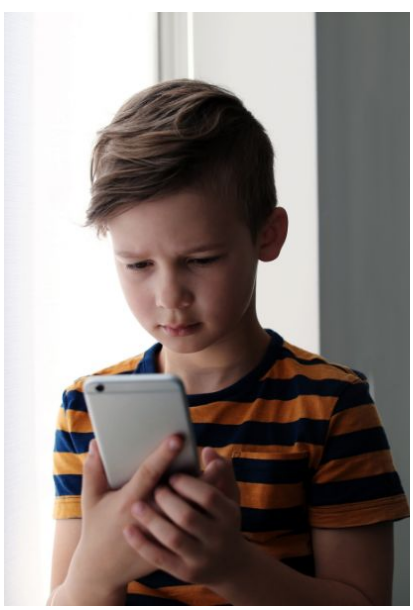
Está en tu mano prohibir el acceso a **páginas que estén calificadas para mayores de 18** años. Entre ellas, destacan las webs de **contenido inapropiado, violento o incluso videojuegos no aptos para menores de edad**. Cuando intenten entrar a uno de estos sitios, el navegador lo bloqueará automáticamente.

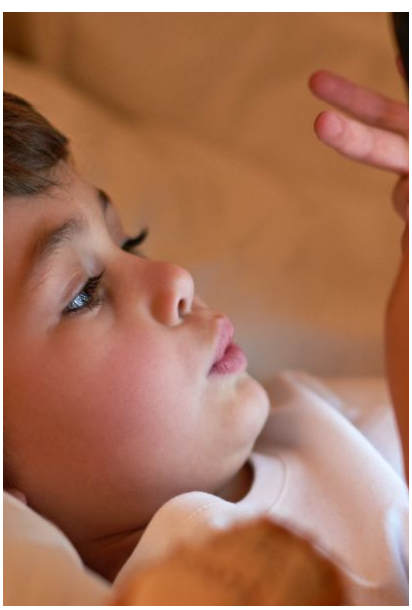
Garantizar el uso saludable

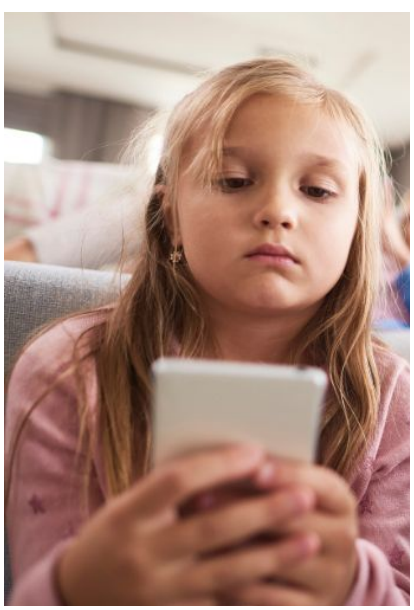
Como ya sabrás, es fundamental que las personas menores de edad aprendan a **equilibrar el tiempo que dedican al uso de la tecnología** y a otras tareas, como el estudio o el descanso. A veces, alcanzar ese equilibrio no es fácil, pero puedes ayudarles a conseguirlo mediante el **bloqueo de los dispositivos electrónicos a ciertas horas** del día.

Supervisar la navegación

Si tus hijos o hijas acostumbran a utilizar Internet, puedes **supervisar las páginas que visitan en la red para detectar posibles riesgos**. Esta función puede ser un útil complemento a la restricción de determinadas páginas. De esta manera, recibirás un informe en tu dispositivo con los sitios web en los que han estado y te mantendrás alerta ante los riesgos de la red.







Bloquear llamadas y contactos

Con tu teléfono, tienes la posibilidad de **poner un filtro a las llamadas que hacen y reciben tus hijos e hijas**. Con ello evitarás que tengan contacto con personas desconocidas y, a su vez, impedirás la comunicación con determinados contactos en WhatsApp y otras plataformas de mensajería instantánea. Es una medida muy útil para evitar posibles situaciones de acoso.

Recibir una alerta

Tienes la opción de activar una función denominada «Botón del pánico», «Botón de emergencias» o «Botón SOS», entre otros. Esto te permite **establecer contacto con tu hijo o hija de forma inmediata en caso de urgencia**. También le puede servir para **enviarte su ubicación y hacer una llamada si está en peligro.**

Para activar esta función deberás acudir a la pestaña de 'Ajustes' del dispositivo. Allí encontrarás un apartado de 'Contraseñas y seguridad' y, dentro de este apartado, la opción 'SOS de emergencia'. En caso de necesidad, tu hijo o hija podrá enviar un mensaje de texto con su ubicación e incluso con su historial de llamadas durante la última hora a los contactos definidos como 'Contactos de emergencia' pulsando el botón de encendido 5 veces seguidas.

Aunque la forma de activar la función puede variar ligeramente de un dispositivo a otro, en el mismo apartado de 'SOS de emergencia' te explicarán el número de veces y los botones a pulsar para enviar la señal. Es importante que repases esa información con tu hijo o hija para asegurarte de que, en caso de urgencia, sabe cómo actuar.

¿Cuáles son las principales herramientas de control parental?

Vamos a hacer un repaso por las principales *apps* de supervisión. Hemos incluido opciones dirigidas especialmente para personas usuarias menores de edad que resultan seguras y efectivas.

Family Link

Esta primera opción pertenece a Google y es una aplicación destinada a **facilitar el uso de una Internet segura a menores de edad**, pero siempre dentro de unas normas básicas. En este caso, se establece un vínculo en tiempo real entre el *smartphone* de tu hijo o hija y el tuyo, lo cual te ayudará a saber qué están haciendo por medio de informes continuos. Hay cuatro funciones principales:

1. **Recibir recomendaciones**. Como la variedad de programas disponibles en la red es muy amplia, recibirás sugerencias de personal docente con contenido infantil. Así, tendrás acceso a un listado por temáticas de opciones que pueden descargar para aprender o simplemente para divertirse.
2. **Conocer su actividad**. Cada día, recibirás un informe que detalla las aplicaciones que han estado utilizando y su duración. De esta forma, podrás valorar si están haciendo un uso responsable de su tiempo frente a las pantallas y prevenir posibles casos de dependencia tecnológica.
3. **Limitar el uso del dispositivo**. Puedes bloquear el acceso a ciertas aplicaciones o directamente ocultarlas para que no sepan de su existencia. También recibirás notificaciones cada vez que quieran hacer una descarga, con la potestad de autorizarlas o denegarlas según creas conveniente.
4. **Controlar el tiempo**. Para evitar que utilicen el móvil durante los momentos de descanso o estudio, puedes establecer una franja autorizada. Fuera de ese tiempo, el aparato permanecerá bloqueado hasta que tú lo autorices. Del mismo modo, esta función te permite ajustar su bloqueo cuando hayan pasado determinadas horas seguidas con un dispositivo.

Una característica muy interesante de esta herramienta es que facilita conocer la ubicación de los más pequeños mediante Google Maps. Esto es ideal cuando alcanzan cierta edad y necesitan ganar algo de independencia en sus trayectos hacia el colegio o a casa.

Apple en familia

Si tienes un dispositivo de iOS, puedes establecer una conexión en tiempo real con tu hijo o hija. Esta funcionalidad se activa fácilmente desde los ajustes de tu teléfono, **su uso es bastante sencillo y fomenta la interacción *online* entre la familia**, con un máximo de seis miembros.

Apple en familia está más enfocada a **crear un entorno colaborativo**, siempre con control hacia menores de edad. Tienes la opción de configurar un grupo de personas (y dispositivos) para proporcionar un espacio en común, donde cada persona desarrolla un rol configurado previamente:

- **Organizador**. Quien controla el grupo y añade miembros. Dispone más poderes y libertad de acción que los demás. Generalmente, suele ser el padre o la madre.
- **Padre / Tutor**. Lo más frecuente es que este rol lo ejerza el otro adulto. Tiene también plena libertad de acción, aunque no lleva a cabo la gestión del grupo.
- **Menores**. En estos casos, el teléfono no les asigna un nombre en sí, sino que expone directamente su edad. Sus acciones son controladas por los dos roles anteriores, quienes se encargan de garantizar su seguridad.

Una vez formado el entorno familiar, cada integrante gestiona qué desea compartir con los demás, llevando a cabo las siguientes acciones:

- **Crear un álbum familiar**. A través de las imágenes que se van añadiendo a la galería, es posible combinarlas.
- **Difundir música**. La totalidad de sus integrantes pueden crear una lista de reproducción añadiendo sus temas favoritos.
- **Compartir almacenamiento**. Es posible adquirir un plan de almacenamiento para toda la familia para guardar todo tipo de documentos, imágenes y vídeos.
- **Sincronizar**. Esta función es compatible con otros productos de la marca Apple, como la televisión o el reloj.

Estas opciones son ideales para los más pequeños, ya que evita que hagan un uso aislado de dispositivos como el teléfono móvil o el ordenador. Del mismo modo, hay tres acciones principales disponibles para supervisar su actividad en la red:

1. **Limitar el uso**. A través de la función «Tiempo de Uso», podrás delimitar las horas que pasan con sus móviles u ordenadores. También puedes asignar un límite para cada tipo de actividad (juegos, navegación, etc.).
2. **Observar la ubicación**. Sabrás dónde está cada miembro de la familia instantáneamente, incluso si no tiene conexión.
3. **Evitar compras no deseadas**. Cada vez que vaya a realizar una compra, recibirás un mensaje en tu dispositivo para autorizarla, conocerás la cantidad de dinero necesaria y el nombre del producto que quiere adquirir.

Como has podido ver, el **control parental** es la mejor forma de garantizar un espacio seguro para los internautas más jóvenes. La clave está en darles libertad, pero siempre dentro de un entorno vigilado.

vuela

3.7

Consejos para que puedas hacer un pago por Internet de forma segura

Hoy en día, las **compras por Internet** siguen ganando popularidad. Sin embargo, el auge de esta modalidad comercial no ha hecho que desaparezca la necesidad de tomar algunas **precauciones cuando realizamos pagos en el entorno *online***.

Por ello, todos y todas podemos poner de nuestra parte para evitar que quienes delinquen en la red se lucren con el comercio del siglo XXI. **¿Cómo puedes hacer que el pago por Internet sea completamente seguro?**

Junta de Andalucía

Agencia Digital de Andalucía

¿Es seguro pagar por Internet?

Esta es una de las preguntas más comunes que surgen a la hora de comprar *online*. No se puede concebir Internet como un lugar peligroso, porque no lo es. Todo depende de que tomemos las debidas precauciones y evitemos los entornos de mayor riesgo. Así, haremos un uso seguro y cómodo de las tecnologías.

Pagar por Internet resulta completamente seguro si lo hacemos de un modo correcto. Para ayudarte a conseguir este objetivo, te proponemos un método que hemos llamado **«las tres S de los pagos por Internet»**: seleccionar, supervisar y suprimir.

Seleccionar

Que una web ofrezca la posibilidad de efectuar pagos no significa que sea segura. Nada más lejos de la realidad. La clave está en **seleccionar las páginas que resultan de confianza** y las que no. Por ejemplo, las plataformas bancarias, las tiendas *online* con mayor reputación o la Administración Pública.

Supervisar

Cuando vayas a efectuar una transferencia por Internet, presta mucha atención al proceso y **supervisa el entorno** para comprobar que dispone de diversos certificados de seguridad (más adelante te explicaremos cuáles son). Además, hay que **examinar la web** para asegurarnos de que no hay contenido sospechoso, que el pedido es el correcto y que el precio es el acordado.

Suprimir

Cuando compras por Internet, tu motor de búsqueda te pregunta habitualmente si quieres **guardar los datos de tu tarjeta**. Si lo haces, estos se quedarán anclados a tu cuenta de Google/iOS y a tu dispositivo. Esto **no es para nada recomendable**, así que suprímelos siempre o, directamente, no autorices que se almacenen.

¿Qué alternativas puedes utilizar para hacer una transferencia?

Si necesitas llevar a cabo una transacción *online*, tienes la posibilidad de recurrir a distintas **plataformas, aplicaciones y páginas**. De este modo, puedes **enviar y recibir dinero o comprar** de un modo seguro y fiable.

PayPal

Este es el portal más empleado a nivel mundial para realizar pagos por Internet. Básicamente, es una especie de **depósito en el que almacenas dinero para pagar *online***.

PayPal ofrece una ventaja significativa: realizar las compras a través de este depósito *online* **sin la necesidad de introducir tu cuenta bancaria ni tu tarjeta de crédito**. Solo tendrás que transferir el dinero deseado desde el banco hasta tu cuenta de PayPal y, una vez ahí, usarlo como lo estimes más oportuno.

Bizum

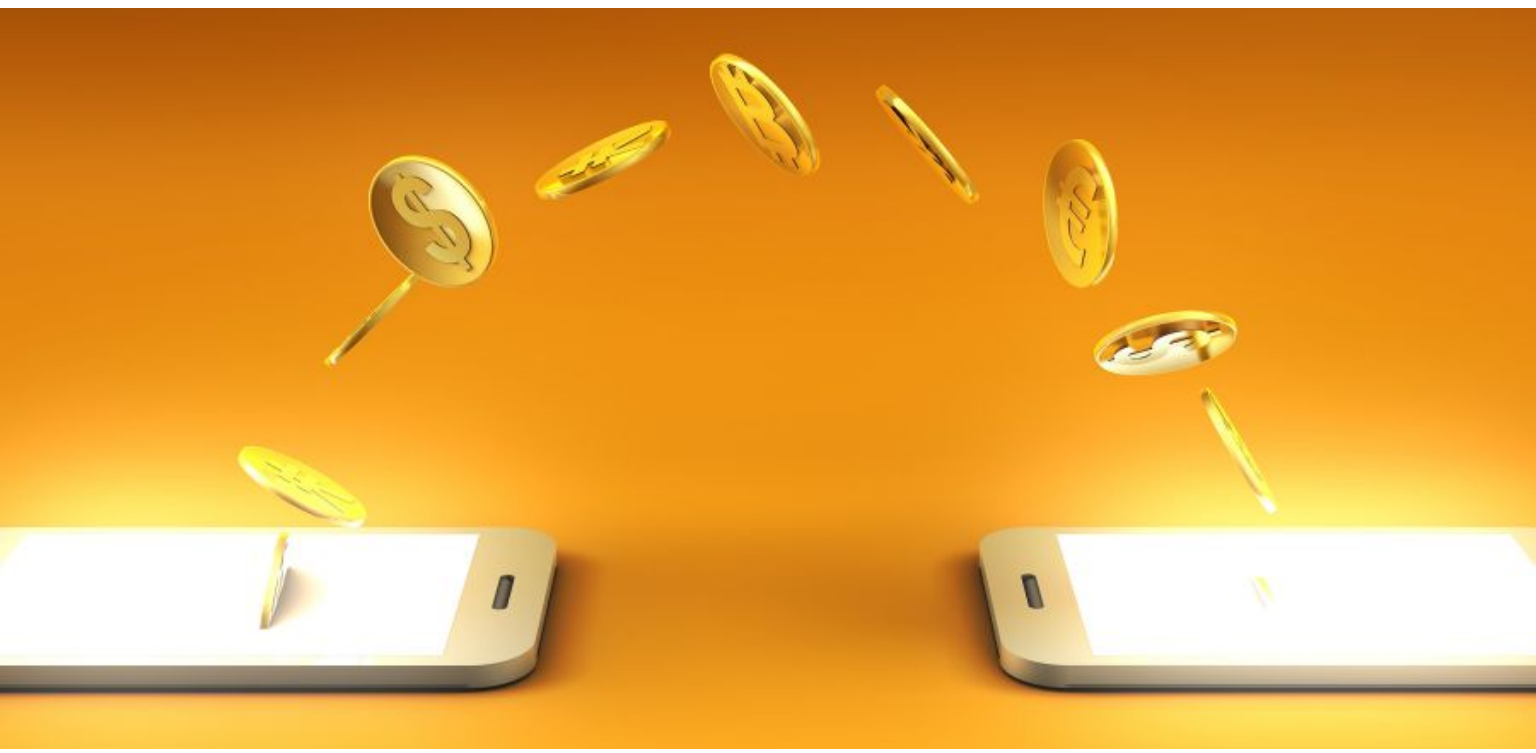
Gracias a su incorporación en las aplicaciones móviles de las entidades bancarias, Bizum ha ganado gran popularidad. Su principal ventaja está relacionada con la facilidad de su uso, ya que te permite **enviar dinero desde tu cuenta bancaria a los contactos de tu teléfono**. De la misma forma, también puedes hacerlo poniendo el **número de la persona destinataria de la transferencia**.

Dispone de un excelente nivel de seguridad, por lo que tienes la garantía de no sufrir ningún tipo de problema. A su vez, te sirve para efectuar pagos por Internet en la mayoría de tiendas *online*, e incluso para cobrar un premio, como la lotería.

Redsys

Desde siempre, Redsys ha sido la principal vía de pago electrónico en España. **Es ideal para proteger tus datos, ya que ni la propia tienda tiene acceso a ellos**. Por tanto, es otra de nuestras recomendaciones para que hagas tus pagos por Internet. La mayoría de las páginas web incorporan esta aplicación de transacciones.

Frecuentemente la habrás oído bajo el nombre de **«pasarela de pago»**, sobre todo en la Administración Pública. Sin embargo, aunque hay muchas pasarelas de este tipo, Redsys es la más empleada. Está vinculada con las principales entidades bancarias de nuestro país y **es compatible con la tarjeta de crédito y débito**.



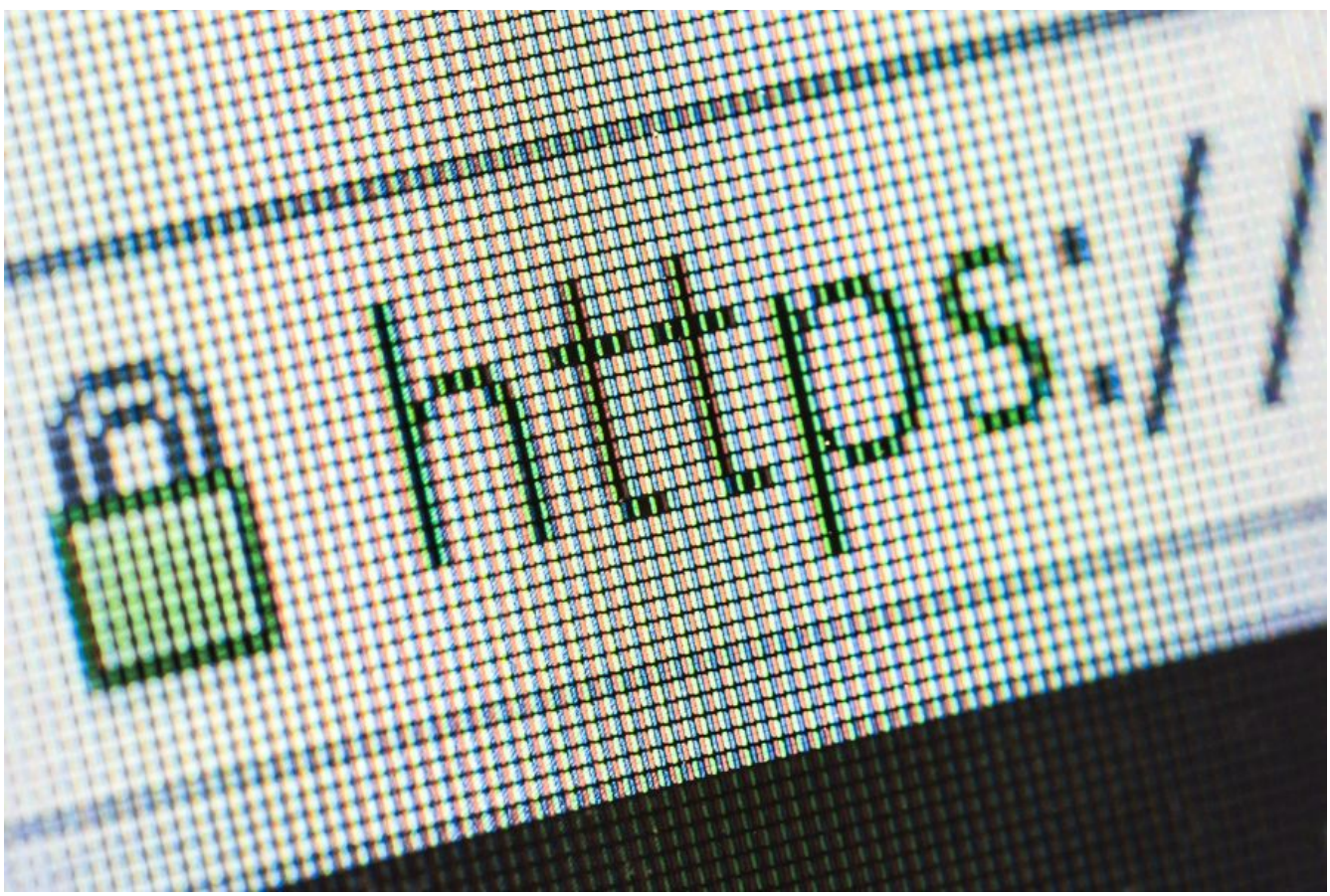
¿Cómo identificar una web segura para hacer un pago?

Además de las opciones que te hemos mostrado, también tienes la **posibilidad de pagar directamente con tu tarjeta.** En este caso, no se usan depósitos *online* como intermediarios, sino que el dinero sale de tu cuenta corriente y accede a la web de forma directa. En este caso, **primero debes asegurarte de que la web es segura**.

1. Verificar la fiabilidad de la página

Antes de saber si una página es segura para hacer un pago, primero debes corroborar que sea fiable. **Dispones de varios métodos para comprobarlo**:

- Revisa que aparezca el **icono de un candado en la barra de direcciones** de tu navegador web (Chrome, Firefox, Internet Explorer, etc.), al lado del enlace (cuando estés dentro de la web).
- Busca la **denominación «https»** (no http) en el enlace para garantizar el cifrado y la protección de tu información.
- **Utiliza un antivirus** para detectar cualquier amenaza o brecha de privacidad automáticamente.



2. Verifica la compra

Si vas a comprar en una tienda *online*, primero **revisa tu pedido**. **Desconfía de aquellas ofertas sospechosamente atractivas o de productos que tengan malas opiniones** entre sus compradores (importante: lee los comentarios). **Tampoco confíes en páginas que tengan un aspecto poco profesional.**

Una vez que tengas tu pedido revisado, comprueba que los artículos son los adecuados y que su importe es el que tenías en mente. **Presta especial atención a los gastos de envío**, que pueden ser considerablemente altos en ocasiones y **analiza el precio final** para descartar fraudes o engaños.

3. Evita las formas de pago sospechosas

Cuando efectúes el pago, elige métodos como los que te hemos propuesto antes (PayPal, Bizum o Redsys, principalmente). **Nunca utilices formas de pago que no conozcas. Tampoco optes por BTC** (*bitcoin* o criptomonedas) a no ser que se trate de un sitio web de tu confianza.

En resumen: **nunca hagas una compra por una plataforma que no te facilite las garantías de seguridad necesarias**. Ante todo, es mejor perder una compra que el control de tu cuenta bancaria y de tu capital.

Además de lo anterior, hay un modo estupendo de comprar con seguridad: **elegir el pago contrareembolso**. Muchos comercios tienen esta opción disponible, donde la transacción se efectúa en el momento en que recibes el producto que adquiriste.

¿Cómo saber si he pagado en un sitio fraudulento?

Lo importante es prevenir, sobre todo, cuando queremos evitar conflictos con ciberdelincuentes. No obstante, es posible que alguna vez hayas hecho una compra por la que te has sentido estafado o estafada. En este caso, hay varias **señales que te ayudarán a saber si has caído en un fraude:**

- **No recibes tu pedido**. Si pasa la fecha límite y no has recibido lo que pagaste, comprueba en primer lugar si se ha producido algún problema logístico que explique el retraso. Si no es así, es probable que nunca existiera tal producto. **Los datos de compra no son correctos**. Si el nombre del comercio aparece de otro modo en la transacción, puede ser una señal de fraude. Lo mismo sucede si el importe no se ajusta a lo que habías pagado.
- **No puedes contactar**. El servicio de atención al cliente es indispensable en todo negocio, especialmente si es *online*. Si no te responden a las llamadas o a tus correos electrónicos, desconfía.

¿Qué debo hacer si detecto un sitio web fraudulento?

Todos y todas tenemos la obligación de comunicar a las autoridades la existencia de un delito, también si se produce en la red. Por tanto, **lo mejor es que informes a la policía de que has sido víctima de un fraude *online***. Para ello, debes comunicar el enlace de la página y otros datos que te puedan requerir.

Si lo prefieres, **la Policía Nacional dispone en su web de un servicio de denuncias anónimas**. Si no has sido víctima del fraude, pero tienes conocimiento de este, comunícalo a las autoridades sin dar a conocer tus datos personales. A la hora de hacer de Internet un lugar más seguro, tu papel puede ser decisivo.

Además de **tramitar la demanda** (o la denuncia), es importante que efectúes **otras acciones** urgentemente:

1. **Si has hecho la compra por otra plataforma** (como PayPal), **desvincúlala de tu cuenta** bancaria y tarjetas.
2. **Informa al banco del fraude** para que pueda **desactivar tus tarjetas** o tomar otras medidas.
3. **Controla el saldo de tu cuenta** para evitar que te roben dinero.

Después de todo esto, habrás cortado la cadena del fraude. **Nunca compartas el enlace del falso comercio** (solo con las autoridades). Además, recuerda que siempre conviene tener un antivirus en el ordenador, *tablet* y *smartphone* para evitar posibles ataques con virus, *malware* y demás.

Ahora que ya sabes **cómo hacer un pago por Internet**, queremos reforzar el mensaje: comprar por Internet es seguro si lo llevas a cabo con responsabilidad.

vuela

Resuelve los problemas más frecuentes

A veces todo lo anterior no es suficiente para evitar ser víctima de un virus, un hackeo o del robo de datos.
En este apartado de la Guía de Ciberseguridad te mostramos paso a paso qué hacer ante un ciberataque.

4

Junta de Andalucía

Agencia Digital de Andalucía

vuela

4.1

Suplantación de identidad en Internet: las claves para responder

La suplantación de identidad es un tipo de ataque cibernético que te puede traer graves problemas. En ocasiones, personas con intenciones maliciosas rastrean información personal que utilizan posteriormente **para hacerse pasar por su víctima** frente a empresas, instituciones o incluso frente a otras personas de su entorno. El lado positivo es que este tipo de ciberamenaza, como la mayoría de los riesgos de la red, puede evitarse con unas sencillas precauciones y el uso de las herramientas de seguridad adecuadas.

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es una suplantación de identidad?

Es una **actividad malintencionada en la que se busca hacerse pasar por otra persona**. Existen diferentes motivos: cometer un fraude, conseguir datos, practicar ciberacoso u obtener un beneficio económico mediante el chantaje. No pienses que solo la sufren las personas famosas o políticas, ya que para evitar ser víctima de este tipo de amenazas lo mejor es no bajar la guardia y mantener siempre ciertas precauciones.

Ten en cuenta que una suplantación de identidad puede realizarse de forma bastante sencilla. Por ejemplo, creando un perfil falso en una red social y actuando como si fuera la persona que dice ser. Esto **supone una amenaza para la seguridad y reputación de cualquiera**, ya que la cuenta que suplanta la identidad podría emitir por ejemplo una declaración difamatoria que afecte al prestigio de la persona afectada o a la desconfianza de quienes conoce.

Además, **la usurpación puede llevarse a cabo a través del robo de la cuenta**. La técnica más sencilla es mediante un ataque de fuerza bruta, que tiene como objetivo descubrir la contraseña probando miles de combinaciones hasta dar con la correcta. Si esta fuera débil, es posible que la persona atacante logre su objetivo y adivine la contraseña. Una vez se haya hecho con el control de la cuenta, podría cambiar la clave de acceso y los métodos de recuperación. Al final, tendría a su disposición cualquier dato o información que contenga la cuenta.

¿Cómo detectar el secuestro de cuentas?

Existen diferentes maneras de detectar que se ha producido un secuestro de cuentas. **Algunas son indirectas, lo que implica que la persona que delinque ha efectuado alguna acción que te involucra**. Por ejemplo, podrías recibir una llamada de una agencia de cobros reclamándote el pago de una deuda a tu nombre, o ver rechazada la concesión de una hipoteca o de un préstamo.

Quizás recibas un correo de confirmación para el alquiler de un piso o que has realizado una compra determinada en una tienda que nunca visitaste. También **es probable que te desaparezca dinero de la cuenta del banco**, si es que el o la delincuente se ha hecho con ella. Y en las redes sociales podrías ver publicaciones en tus perfiles que no has efectuado, como una foto de personas que no conoces o datos de tu vida privada.

Otra forma de detectar la suplantación es tratando de acceder a tu cuenta. Si has probado diferentes métodos y no consigues entrar, puede que estés ante un robo. **Antes de llegar a plantearte esta situación, tienes que haber agotado todas las alternativas**. Considéralo como el último escenario posible, ya que es más probable que hayas olvidado la contraseña.

También **podrías aparecer registrado en numerosas plataformas de Internet** o, directamente, no tener acceso de ningún tipo a las que ya tenías previamente. Por ejemplo, tratas de ingresar en tu cuenta de un sitio de web para visualizar contenido en *streaming*, o de una tienda *online*, y no lo consigues. Agotas todas las opciones de recuperar la contraseña y sigues sin obtener resultados. En este contexto, es probable que te enfrentes a un robo de identidad.

Pasos a seguir en caso de suplantación de identidad

En caso de que la sufras, **no puedes quedarte de brazos cruzados**, pero mantén la calma pues esta situación tiene solución. Además, ten en cuenta que tanto la plataforma en la que se produjo la usurpación como las Fuerzas y Cuerpos de Seguridad del Estado estarán dispuestas a ayudarte. Te recomendamos seguir estos pasos para facilitar una actuación rápida y efectiva:

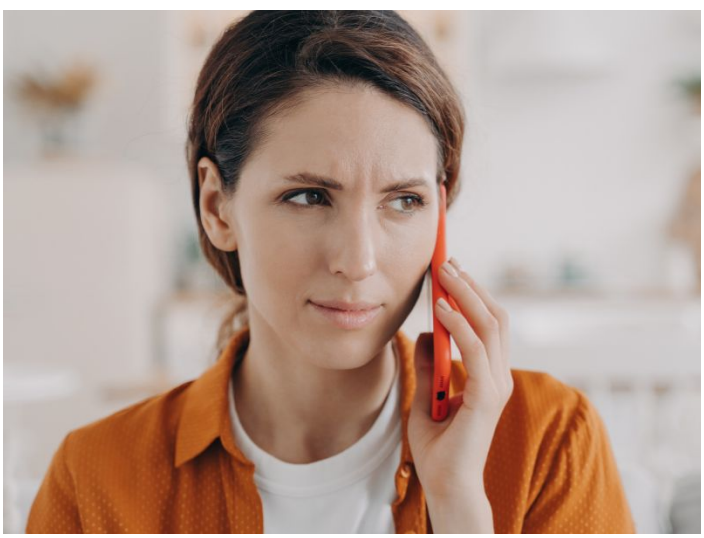
1. Documenta lo que está ocurriendo

Necesitas documentar lo que está pasando antes de denunciar una suplantación de identidad. Procura revisar y agotar todas las opciones que te ofrecen las plataformas para recuperar tu cuenta. Es indispensable que acudas con **pruebas inequívocas de tu situación**. Obtén **copias de posibles correos, mensajes y capturas de pantalla de los actos delictivos**.

En caso de que no tengas éxito en la recuperación y hayas recabado suficientes pruebas, llega el momento de denunciar. Ponte en contacto con las plataformas. Por ejemplo, **en la web de la Oficina de Seguridad del Internauta, encontrarás enlaces a todas las redes sociales disponibles**. Estos te dirigen a las páginas dedicadas a denunciar una suplantación, por lo que tendrás su apoyo en todo momento.

2. Alerta a tus amistades y familiares

Es importante que avises de lo que está sucediendo a tus contactos. **No solo te servirán de testigos de lo ocurrido, sino que les alertarás de que no controlas tus propias cuentas**. De esta forma, evitas malentendidos con quienes aprecias, un problema adicional que puede provocar una suplantación de identidad. Además, podrán ayudarte a mantener el control sobre tu perfil alertando a otras personas.



3. Acude a la autoridad

Si sabes que estás siendo víctima de un caso de suplantación de identidad, no dudes en acudir a la autoridad. **La Policía o la Guardia Civil disponen de unidades especializadas en ciberdelincuencia**. Son especialmente útiles en casos graves en los que no ha sido posible recuperar tus perfiles de otras maneras o **si se cometen delitos utilizando tu nombre**.

Recuerda que las plataformas, como Facebook o Twitter, te permiten denunciar una posible usurpación. Estudiarán tu situación y actuarán en consecuencia, mientras las autoridades investigan lo sucedido y buscan a las personas responsables. Normalmente, recuperarás tus cuentas en poco tiempo.

Pautas para prevenir una suplantación de identidad

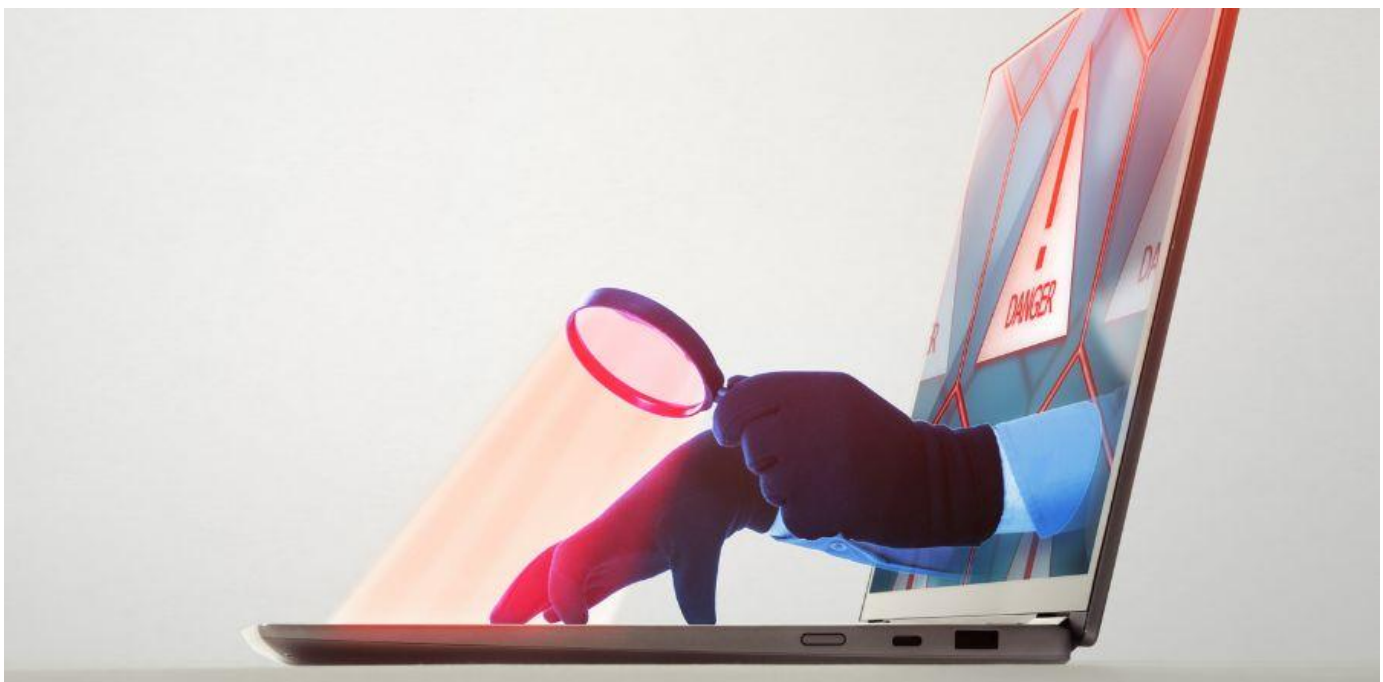
La prevención es la clave para protegerte de una suplantación de identidad. Por suerte, existen diferentes pautas que puedes seguir para ahorrarte este problema tan grave. Además, muchas son sencillas de aplicar, pero de una efectividad indudable.

No muestres tus contraseñas en público

Mostrar tus contraseñas públicamente es un error muy grave. Cualquier persona que quiera hacerte daño, tendrá una oportunidad de oro. No tendrán que realizar mayores esfuerzos para hacerse pasar por ti, ya que saben cómo acceder a tu perfil personal. Esta es una situación que puedes evitar con facilidad teniendo cuidado. Asimismo, si alguien te pide tus credenciales, no las facilites.

Ninguna plataforma te pedirá que le entregues tu contraseña, algo de lo que suelen informar. Así que, ante este tipo de peticiones, la mejor opción es mantener la precaución y no dar dato alguno. Recuerda que la prevención es la clave para navegar de forma segura. **Al igual que no le darías a una persona desconocida la dirección de tu casa, tampoco proporciones tus contraseñas de acceso a tus cuentas**.

Para comprobar si utiliza HTTPS, solo tienes que clicar en su dirección. **Esta debería empezar así: https://**. En caso de que no esté presente, estás en una página insegura y, por tanto, potencialmente peligrosa para ti. Es posible que la persona propietaria no haya activado este protocolo, pero procura prevenir las consecuencias antes de enfrentarte a ellas.



Evita los enlaces extraños

Si un enlace te lleva a una página web con faltas de ortografía, mala presentación o que no cuenta con el protocolo HTTPS, es posible que estés en una que sea falsa. **Los enlaces sospechosos pueden llegar a ti a través de mensajes en las redes sociales, correo electrónico, SMS o WhatsApp**. Si no conoces su origen o el remitente no se identifica adecuadamente, no entres en ellos.

Utiliza sistemas de autenticación de dos pasos

Tu seguridad siempre empieza por tener una **contraseña con un código que sea robusto** (una combinación de mayúsculas, minúsculas, números y símbolos). No obstante, **un sistema de autenticación de dos pasos es el complemento perfecto** para disuadir a cualquier delincuente de acceder a tus cuentas, ya que te otorga una mayor seguridad y tranquilidad al crear varias barreras de protección.

Un ejemplo de este sistema de autenticación es el empleado por los bancos y algunas páginas web. **La primera parte es una contraseña**, la cual debes aportar tú, y **la segunda consiste en un código que se envía a tu teléfono móvil por mensaje SMS**. Esto dificulta que te quiten una cuenta, ya que **es necesario tu dispositivo para verificar el acceso**. También tienes la posibilidad de comprobar tu identidad por correo electrónico, una pregunta de seguridad (cuya respuesta solo conoces tú) y biometría (reconocimiento facial, huella digital, etc.), entre otros. En definitiva, procura **actuar de forma previsora para evitar una suplantación de identidad en Internet**. Estas situaciones pueden complicarse y llevarte a perder tus cuentas en la red. Recurre siempre a las plataformas para buscar una solución y denuncia ante la Policía o la Guardia Civil para evitar males mayores.

vuela

4.2

¿Has sido víctima de un fraude con tarjeta de crédito? Cómo actuar

En ocasiones, una oferta especialmente tentadora puede hacer que bajemos la guardia y dejemos de realizar las **comprobaciones de seguridad necesarias antes de comprar en un sitio web.** En la mayoría de los casos esta situación se quedará en un comportamiento de riesgo sin que suponga un mayor problema, pero es posible que tengamos la mala suerte de toparnos con una página web fraudulenta y nuestros datos bancarios se encuentren en peligro. Llegados a ese punto, **¿qué puedes hacer si has sido víctima de un fraude con tu tarjeta bancaria?**

Junta de Andalucía

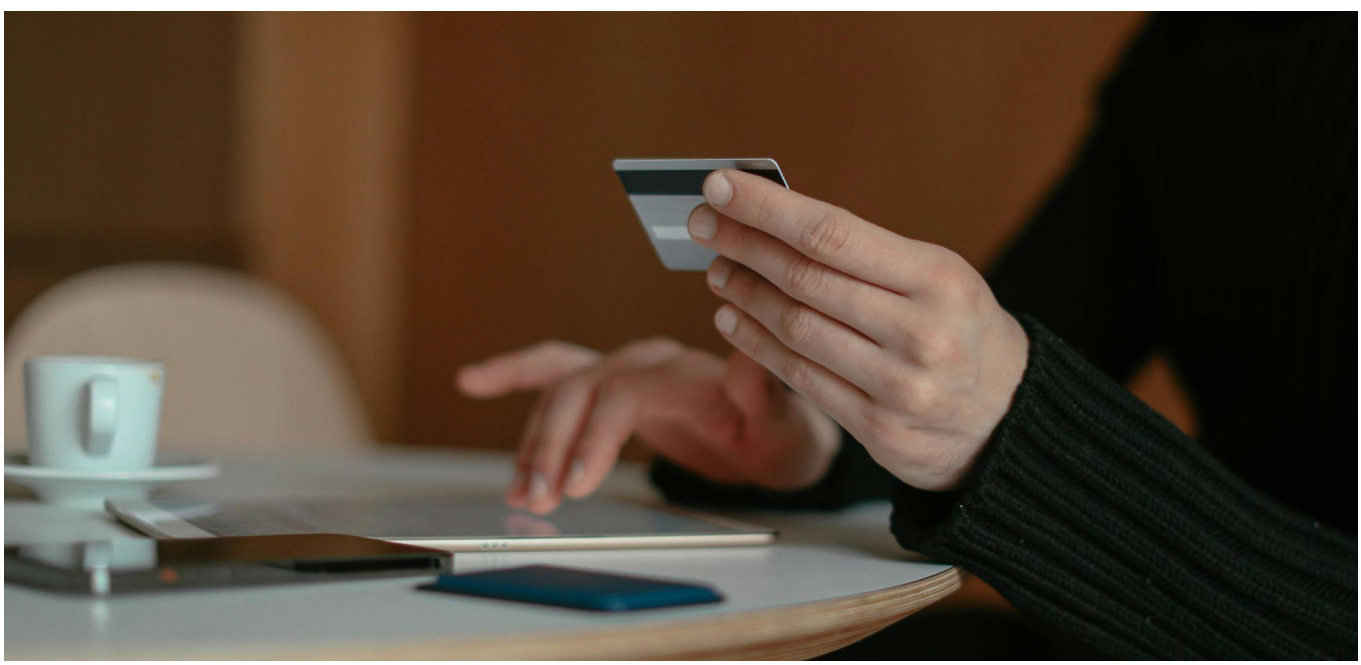
Agencia Digital de Andalucía

¿Cómo saber si hemos comprado en una página web no segura?

Existen varios métodos que te ayudarán a saber si un sitio web es poco recomendable en apenas unos segundos. Además, estas pautas de seguridad puedes y debes aplicarlas antes de finalizar una compra *online* para prevenir posibles riesgos. En caso de que ya hayas comprado en el portal, puedes recurrir a ellas para verificar que todo está en orden.

Antes de comenzar, cabe hacer una aclaración: **que una página web sea poco segura no significa que sea una página web fraudulenta**, pero deberemos tener especial cuidado en cualquiera de los dos casos. Entonces, ¿cuál es la diferencia? Si has comprado en una página web no segura es probable que recibas el envío con normalidad; es decir, el funcionamiento de la empresa puede ser corriente, el riesgo está en que el sitio web **no garantiza que tus datos están protegidos correctamente**, por lo que cualquier persona (más allá de las propietarias del portal) tiene la opción de acceder a estos.

En contraposición, si has comprado en una página web fraudulenta lo más seguro es que no recibas ningún pedido y esa sea la primera señal de alerta. Normalmente, detrás de estas páginas no hay un negocio, sino personas que buscan realizar cualquier tipo de **ataque contra nuestros equipos o la información que se encuentra desprotegida.** Aquí el riesgo será aún mayor.



Dirección

Si revisas el enlace de la página, verás si dispone de un nivel mínimo de protección. Para ello, **verifica que aparece la denominación «https»** (no «http») al principio de este. De este modo, sabrás que, como mínimo, cumple con lo básico en materia de ciberseguridad: tu información estará codificada y protegida.

Certificado de seguridad

Cuando estés dentro de la página, **comprueba si aparece el icono de un candado justo antes del enlace**. Si no está presente, la web carece de un certificado que garantiza que es un sitio seguro. Por tanto, estás ante otra de las señales que te deberían hacer desconfiar y tomar medidas.

Es importante hacer un inciso: este certificado cabe la posibilidad de que no esté disponible en todo el portal en el que has comprado. Muchas tiendas *online* solo protegen las secciones en las que se producen las ventas. Esto no es del todo recomendable, pero al menos garantiza que tus transacciones están cifradas (es decir, que se han blindado con un código).

Aviso legal

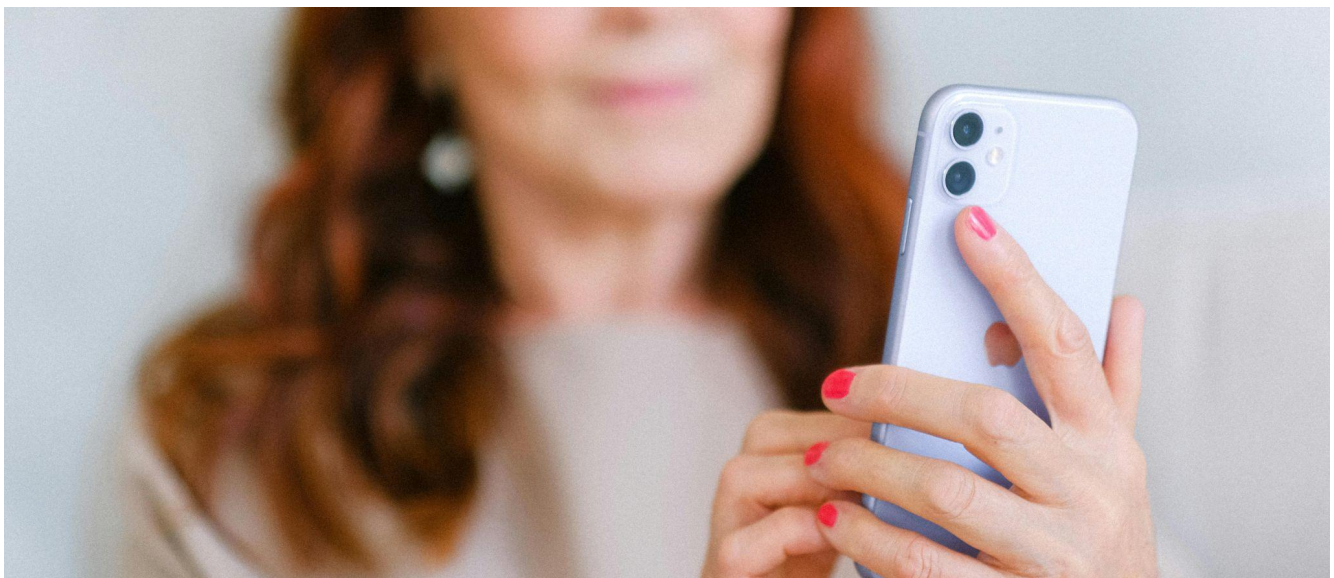
Por ley, todas las páginas web están obligadas a exponer un apartado de aviso legal. A través de este, **sabrás quién es la persona propietaria del portal y otros datos de interés**. Incluso si la página en la que has comprado lo tiene, observa que no aparezca información sospechosa y puedas identificar fácilmente a la empresa que hay detrás del sitio web. Encontrarás el aviso legal, generalmente, en la parte inferior de la tienda.

Información demasiado llamativa

Si has adquirido un producto con un descuento muy elevado, desconfía. En este sentido, son muy comunes los supuestos teléfonos móviles que se anuncian a precios fuera de mercado. Aunque cada vez son más las marcas que apuestan por una estrategia de descuentos o agilizar los tiempos de envío como reclamo, te recomendamos que apliques el sentido común para identificar posibles estafas. Por ejemplo, un artículo que se entrega en el día pese a proceder de países extranjeros puede resultar un timo, para salir de dudas lo mejor es que compruebes detenidamente todas las condiciones de entrega y verifiques las opiniones de otros usuarios.

Origen

Que una página web sea extranjera no significa que no sea fiable. Sin embargo, en algunos casos es posible que no se ajuste a las exigencias de ciberseguridad en España o en la Unión Europea. Por tanto, no esperes un nivel de protección similar al que tienen los portales que cumplen nuestra legislación nacional o comunitaria. Esto deberás tenerlo especialmente en cuenta en relación a la protección de tus datos personales.



¿Qué hago si he comprado en una página web no segura? ¿Puedo recuperar el dinero?

Lo primero que has de saber es que hay solución. Si efectuaste un pago en una tienda *online* sospechosa, actúa rápido para minimizar los posibles riesgos. Y es que, dependiendo de dónde hayas hecho la transacción, te podrás enfrentar a situaciones como las siguientes:

- **Robo de información bancaria** (número de cuenta, de tarjeta, titular).
- **Pérdida de dinero** (transacciones involuntarias, robo).
- **Estafa** (recibir una falsificación o directamente no recibir nada).

Vamos a mostrarte un orden de pasos que te recomendamos seguir ante un incidente de este tipo.

1. Comunicárselo a tu banco

Lo primero de todo es comunicárselo a tu banco. Es importante que lo hagas rápidamente **para que te indiquen los pasos a seguir a partir de ese momento**. Necesitarás proporcionarles el importe total de la transacción, el nombre del comercio y los datos relativos a la fecha y hora de la compra.

2. Bloquear la tarjeta bancaria

Lo más probable es que el banco lo haga desde que le comuniques lo que ha sucedido. En caso contrario, solicita que lo realicen inmediatamente (en función de tu entidad, tienes la opción de hacerlo tú desde su aplicación móvil o página web). Bloquear la tarjeta, ya sea de débito o de crédito, implica que **el comercio no puede realizar transacciones no autorizadas por ti.**

3. Poner una reclamación

Aunque la web no sea segura, es posible que se trate de un comercio real. En tal caso, **pon una reclamación para que te devuelvan tu dinero y cancelen tu compra**. Si no recibes respuesta o esta es negativa, acude a la Oficina de Atención al Consumidor de tu localidad, a Consumo Responde o a Confianza Online, que agrupa a un gran número de comercios electrónicos.

4. Denunciar ante las autoridades

Este paso es imprescindible, incluso aunque hayas llevado a cabo los anteriores con éxito. Como internautas, tenemos la obligación de comunicar cualquier indicio de delito a las autoridades. La Guardia Civil dispone de un portal donde interponer denuncias relacionadas con estafas *online* mediante varias vías de comunicación.

5. Proteger a tu círculo cercano

Si has llegado a esa tienda *online*, es muy posible que haya sido por recomendación. En tal caso, advierte a la persona que te la enseñó para evitar que caiga en la misma trampa. Haz lo mismo con tus familiares y amistades. **Todos y todas podemos cortar el círculo de las estafas digitales**.

6. Eliminar toda relación con la página web

Este último paso te ayudará a evitar futuras estafas en el futuro. Borra todo tu rastro de la página web fraudulenta, lo que incluye eliminar tu cuenta (no cerrar sesión, sino eliminarla directamente). Para ello, **ponte en contacto con el portal y solicita tu «derecho al olvido»**.

¿Cómo puedo evitar que me vuelva a suceder en el futuro?

Muchas personas cogen miedo tras sufrir una mala experiencia en Internet, sobre todo si está relacionada con transacciones bancarias. Sin embargo, esto no es motivo para dejar de comprar por la red. La clave está en hacerlo con seguridad, entonces podremos disfrutar de todas las oportunidades que nos ofrece el mundo digital con total tranquilidad.

En ese sentido, para evitar futuros percances de este tipo, te proponemos una serie de recomendaciones que harán que tu experiencia de compra *online* sea totalmente satisfactoria.

1. Crea una lista de confianza

Te ayudará tener una lista de comercios donde las transacciones sean seguras. Para ello, **básate en tu propia experiencia o pide opiniones a personas de tu entorno**. Si quieres averiguarlo con mayor facilidad, te recomendamos revisar que la tienda esté inscrita en Confianza Online, una organización sin ánimo de lucro dedicada al *ecommerce* fiable.

2. Abre una cuenta para compras por Internet

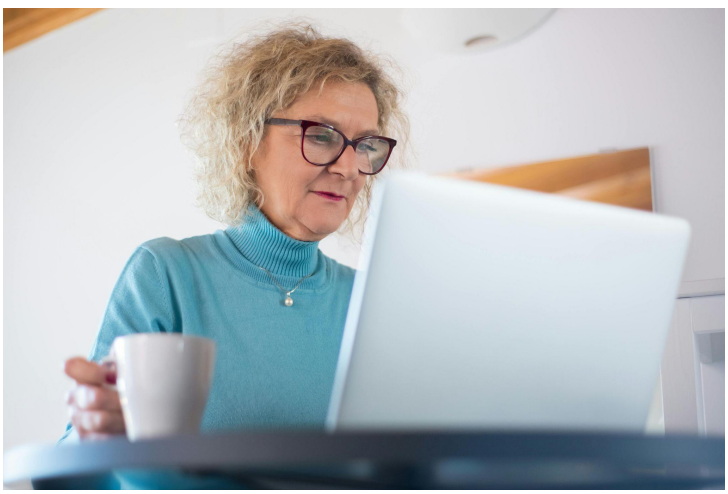
¿Sueles realizar tus pagos a través de tu cuenta principal? Lo más aconsejable es que abras una exclusivamente para las tiendas *online*. De este modo, tendrás la opción de dejarla siempre sin saldo y **añadirás la cantidad necesaria para la compra en el momento** de efectuarla. Muchas entidades bancarias de nuestro país disponen de planes para este tipo de operaciones.

3. Comprueba siempre los métodos de pago

Este tercer consejo ponlo en práctica cuando hayas comprobado que la web es segura. En este sentido, es importante que prestes atención a los métodos de pago que tienes a tu disposición. **Desconfía si aparecen varios y solamente está disponible uno**, ya que es un indicio de que quieren conducirte a una sección específica donde extraer tus datos.

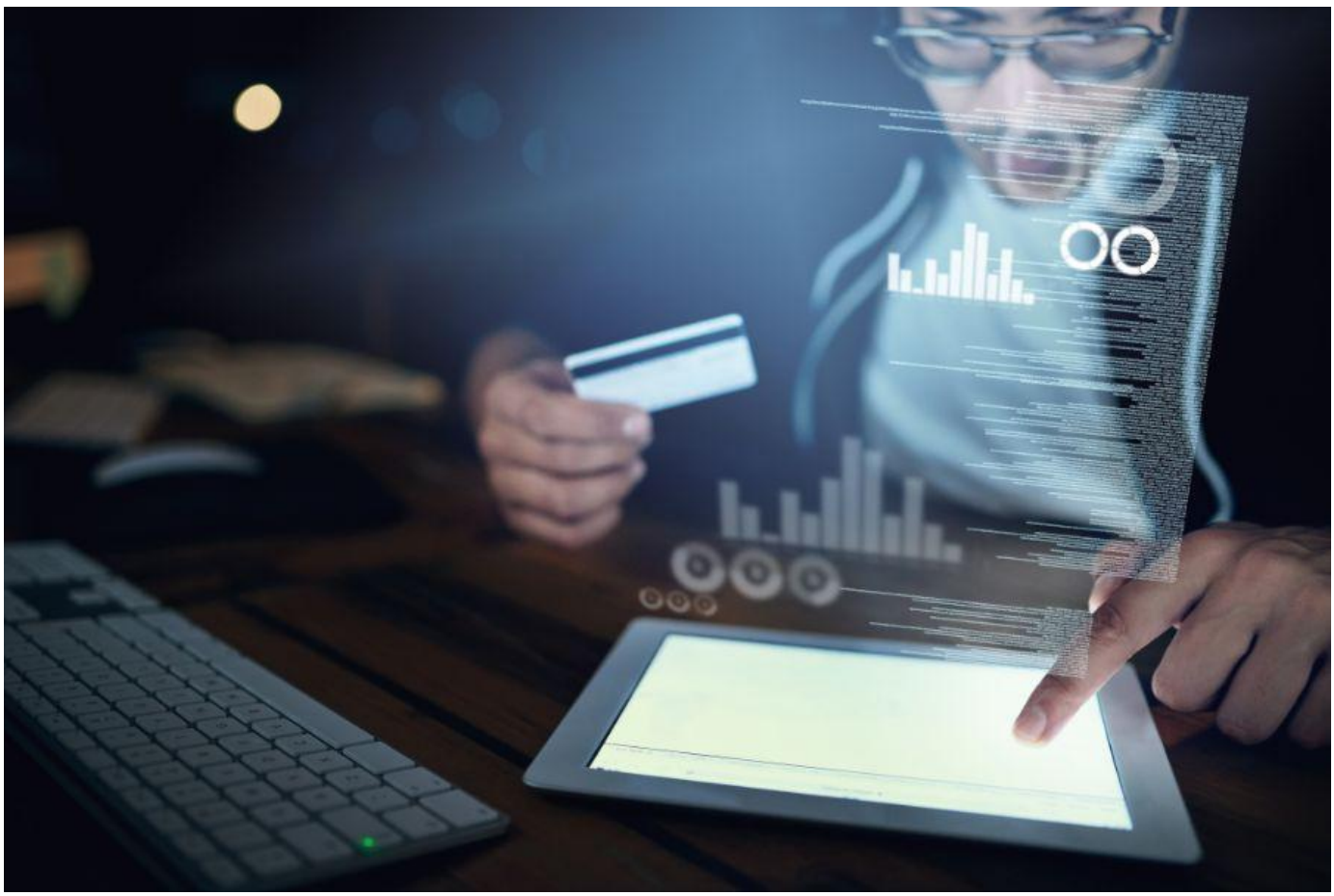
4. Elige vías de pago seguras

Relacionado con lo anterior, hay varias formas de pago que te ayudarán a hacer una transacción con seguridad. **La principal es, obviamente, a través de tu tarjeta bancaria**. No obstante, también tienes la posibilidad de tramitarla por medio de Redsys o PayPal, entidades de ámbito internacional que cifran sus datos adecuadamente, o realizar tus compras contra reembolso. Evita Western Union y similares. Puedes aprender más sobre métodos de pago seguros en este artículo.



5. Compara los precios

Para no caer en la trampa de las ofertas demasiado llamativas, es necesario que compares siempre los precios. De esta manera, **te harás una idea del coste medio que tiene el producto** que vas a adquirir. Si la realidad no se parece a lo que ves en la web, no hagas la compra. Con toda seguridad, se tratará de un engaño.En definitiva, **puedes protegerte incluso si ya has sido víctima de un fraude con tarjeta bancaria**. La clave está en realizar un uso responsable de las redes y ayudar a hacer de estas un espacio más protegido. Nadie duda de que las compras *online* son el futuro, pero estas deben ser seguras y fiables.



vuela

4.3

Cambiar todas las contraseñas: cómo actuar en caso de *phishing*

Si has sido o crees que puedes ser víctima de *phishing*, lo primero que debes hacer es **cambiar todas las contraseñas de tus cuentas y perfiles digitales.** Esto te permitirá frenar la amenaza mientras tomas otro tipo de medidas, como la comunicación con tu banco o la denuncia de tu caso ante la policía o guardia civil. A continuación, te explicaremos los pasos que debes seguir para minimizar los daños de un ataque de *phishing*, pero, primero veamos en qué consiste este tipo de ataque cibernético.

Junta de Andalucía

Agencia Digital de Andalucía

¿Qué es el *phishing?*

El *phishing* es un tipo de ciberamenaza que nos podemos encontrar al navegar por el ciberespacio y se basa en captar datos personales de sus víctimas, como sus cuentas y contraseñas, mediante algún tipo de engaño o estafa. Por ejemplo, mediante el envío de un sms o correo electrónico haciéndose pasar por tu banco o por tu empresa de suministro de energía.

Estos *emails* incluyen **enlaces hacia sitios web preparados** para conseguir tu información privada. Lo que hacen es imitar a la empresa legítima y te solicitan algunos datos personales con indicadores de urgencia para crear cierta alarma y actúes con prontitud. Estos ataques guardan una estrecha relación con el ***spam,*** por lo que tendrás que tener un especial cuidado con este tipo de mensajes. ¿Por qué? Estos *emails* o *sms* acostumbran a enviarse masivamente para multiplicar el número de víctimas potenciales.

¿Cómo detectar si estoy sufriendo este ataque?

Este tipo de acciones cuentan con una estrategia muy definida. Sin embargo, no hay que alarmarse, ya que si sigues los pasos adecuados, podrás detectarlos sin problema. Pese a que estos mensajes tienen una apariencia normal de alguien en quien confías, siempre hay **una serie de indicios que te ayudarán a identificar un caso de *phishing***.

En el mensaje es muy común que se utilice algún **discurso alarmista**. Por ejemplo, que se ha detectado un inicio de sesión sospechoso en su sitio web, o bien pedirte que hagas clic en un enlace para realizar un pago pendiente. En otros casos, te ofrecen un cupón para aprovechar un descuento o te indican que hay algún tipo de problema con tus datos personales y necesitan que los verifiques. Además, es poco habitual que un mensaje corporativo de una empresa que hayas contratado vaya a la carpeta de correo no deseado. Por tanto, los *emails* que recibas en esta carpeta es recomendable tratarlos con cuidado.

Si ya lo estás sufriendo porque desconocías cómo identificarlo, algunos indicadores te ayudarán a darte cuenta de esta situación. En el caso de que tus contactos te avisen de que están recibiendo correos desde tu cuenta con mensajes «raros», lo normal es que estés siendo víctima del *phishing*. Seguramente tengas algún programa malicioso en tu ordenador que sea el causante de esos envíos. Otras pruebas son los cargos realizados a tu cuenta bancaria de compras que no has hecho o publicaciones en tus perfiles de redes sociales que no has efectuado. Y si intentas entrar en una página web con tus credenciales y dice que tu código de acceso no es válido, también puedes sospechar de que algo no marcha bien.

¿Cómo resolver con éxito este ataque y minimizar los daños?

Lo primordial es mantener la calma. En este sentido, el primer paso a llevar a cabo es averiguar los datos que hayan podido ser filtrados y conocer así cuáles son las amenazas reales. Posteriormente, es **necesario actuar para evitar que se pueda repetir esta situación** y proteger tu privacidad. Recuerda que las contraseñas son tu primera barrera de seguridad contra los y las ciberdelincuentes, por lo que también deberás ocuparte de ellas lo primero para devolver la protección a tus dispositivos.

A continuación, te exponemos un paso a paso para neutralizar cualquier ataque que hayas sufrido.

Cambia la contraseña de tu correo electrónico…

Una de las primeras medidas que es recomendable realizar es cambiar las contraseñas de tus cuentas de correo electrónico, ya que es una información básica común de todas tus otras cuentas (bancos, tiendas, etc.). Para ello, inicia sesión con normalidad y en los ajustes de tu servidor de mensajería, entra en el apartado de «Cuentas e importación» si utilizas Gmail, y cámbiala; en caso de utilizar otra aplicación de correo electrónico, esta opción estará en el apartado de Cuenta o Configuración. Basta con escribirla dos ocasiones para verificar que la introduces correctamente y el proceso finalizará. ¿Y si no la recuerdas o el ciberdelincuente la ha modificado? En ese caso, **inicia un proceso de recuperación para posteriormente modificarla**.

Existen dos opciones para poder recuperar una contraseña. Para ello, necesitarás haber facilitado previamente un número de teléfono móvil o un *email* alternativo dentro de los ajustes de tu servidor de mensajería. En el primer caso, te preguntará si **estás intentando acceder a tu cuenta de correo electrónico** y te llegará un mensaje SMS a tu *smartphone*, o bien te hará seleccionar una combinación de números. En el segundo, recibirás un mensaje con **un correo de recuperación**. Una vez hayas completado la verificación por cualquiera de estas vías, simplemente tendrás que escribir la nueva clave.

… y las contraseñas de tus redes sociales y otras entidades de relevancia

Además del *email*, tus perfiles de redes sociales son otro de los puntos a vigilar. Modificar las **diferentes contraseñas restablecerá la seguridad que tenías previamente**. Para llevar a cabo este proceso, inicia sesión en cada uno de los perfiles y sigue el proceso que te indiquen.

Asimismo, aplícalo con todos los sitios web en los que tengas una cuenta y sospeches que hayan podido sufrir un acceso malicioso: entidades bancarias, proveedores de telefonía, Netflix, Amazon, etc. Así recuperarás el control y la seguridad.

Utilizar un antivirus

La instalación y el uso de un antivirus es primordial en estos casos. Existen muchos programas especializados que **te protegerán contra estos ataques**. Los antivirus utilizan un sistema de detección de amenazas inteligente capaz de identificar todos los enlaces maliciosos y prevenirte de sus intenciones. Además, también te avisan en caso de que sea el archivo adjunto el que se encuentra infectado.

Una de las opciones gratuitas y accesibles que puedes encontrar es la de **Avast Free Antivirus**. Dispone de todo lo que necesitas para estar protegido y disfrutar de una buena experiencia de navegación. Y si usas el sistema operativo Windows, recuerda que tienes un *software* de seguridad gratuito a tu disposición: Microsoft Defender. Puedes encontrarlo ya instalado en tu ordenador, solo asegúrate de que la protección está activada antes de continuar con la navegación.

Bloquea tus tarjetas de débito o crédito

Otra de las medidas inmediatas si sospechamos que hemos sido víctima de *phishing* es **bloquear todos tus medios de pago, especialmente tus tarjetas**. Esta es la forma de evitar que terceras personas empleen tu dinero en tiendas *online*, por ejemplo. Una vez eliminada la amenaza, te recomendamos que cambies la tarjeta de crédito para asegurarte de que tus datos bancarios quedan totalmente protegidos.

Habla con tu banco y las autoridades

Si has sufrido algún tipo de cobro indebido, **contacta con tu entidad financiera**. Todos los bancos cuentan con equipos especializados en estos temas y podrán asesorarte para evitar que vuelva a ocurrir.

Además, es beneficioso que pongas una denuncia ante la Policía para que puedan investigar tu caso desde su departamento de delitos cibernéticos.

Comunícalo a tu entorno cercano

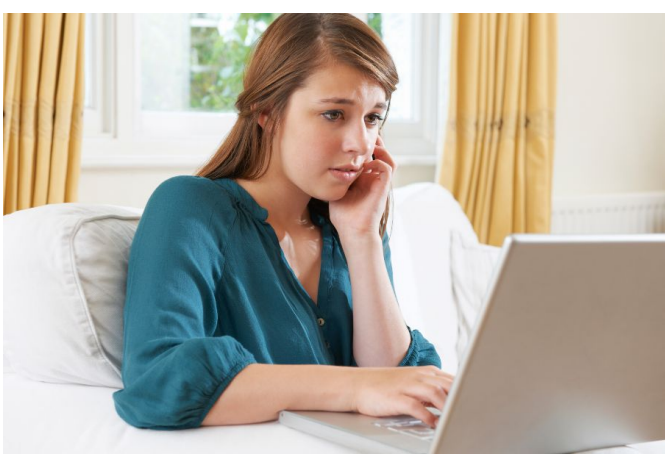
Por último, pero no por ello menos importante, **informa a tu entorno**. De este modo, tendrás la opción de frenar la propagación de esta amenaza. Explícales que has recibido un ataque de *phishing* y que es posible que reciban *emails*, o mensajes por redes sociales, invitándoles a hacer clic en un enlace. Avísales que los ignoren y eliminen.

Consejos para prevenir ser víctima del *phishing*

Existen diferentes acciones que te recomendamos poner en práctica para **prevenirlo** y, sobre todo, tener una experiencia de navegación mucho más segura en Internet. Algunas de las más destacadas son las siguientes:

- **Autenticación en dos pasos:** uno de los métodos más efectivos para poner una barrera a este tipo de ataques, ya que serán necesarios dos dispositivos para verificar tu identidad. Algunos de los más comunes son el teléfono móvil junto al correo electrónico.
- **Sitios web con certificado de seguridad:** es importante que conozcas la fiabilidad de los sitios web donde introduces información confidencial, especialmente cuando compras por Internet. En tu navegador (Google Chrome, Firefox…), fíjate siempre que al lado de la dirección de la página tenga un pequeño candado. Esto indica que los datos están cifrados y, por tanto, seguros.
- **Ante la mínima duda, pregunta:** si recibes un correo o un SMS que sospeches que pueda ser *phishing*, contacta con la empresa. Así, su equipo podrá indicar si se trata de una información válida o un intento de estafa.
- **Usar un gestor de contraseñas:** el uso de esta herramienta también te garantiza un uso seguro de todas las claves que pueden ser de interés para ti. Uno de los más utilizados es el de **Google Chrome**. Desde su última actualización, el servidor te notifica cuando se haya vulnerado alguna y te resultará muy útil en casos de *phishing* para identificar el problema.

Como has podido comprobar, **cambiar todas las contraseñas** es fundamental cuando sufres un ataque de *phishing*. Ahora ya sabes identificar este tipo de amenaza y reaccionar de forma eficaz para resolver el problema y minimizar los posibles daños que te pueda ocasionar.



vuela

4.4

Los pasos a seguir si algún tipo de *ransomware* ataca tu ordenador

El ***ransomware*** es un tipo de programa informático o *software* malicioso que utilizan quienes delinquen en Internet. Cuando infecta una red o un equipo, bloquea la posibilidad de utilizar el sistema afectado, por lo que si resultas víctima de *ransomware*, no podrás acceder a tus archivos personales. Además, te exigirán el pago de un rescate si deseas volver a tener acceso a toda esta información.

Junta de Andalucía

Agencia Digital de Andalucía

Las primeras variantes de este *malware* (*software* con intenciones dañinas) **aparecieron a finales de los años 80**. En aquella época, quienes atacaban exigían que el pago se hiciera por correo postal. Actualmente, las vías más empleadas son las tarjetas de crédito y las criptomonedas. La cantidad suele variar entre cientos y miles de euros, dependiendo de cada caso, como cualquier clase de **secuestro** (de quién sea la persona implicada, la importancia de los datos obtenidos, etc.).

El *ransomware* **se propaga como la mayoría de virus informáticos**. El método más empleado es el envío de correos electrónicos maliciosos, donde la persona usuaria abre algún archivo adjunto o hace clic en un vínculo que la dirige hacia el lugar que desea quien le ataca.

Los diferentes tipos de *ransomware* que hay en la actualidad

Las clases de ***ransomware* más frecuentes** con los que puedes encontrarte son los siguientes:

- **De cifrado**. Está diseñado para cifrar los archivos más importantes que tengas en tu dispositivo. El funcionamiento del equipo sigue con normalidad, sin embargo, tus fotos, vídeos, documentos y demás no podrán abrirse. Por lo general, este *software* muestra un mensaje con una cuenta regresiva en la que te advierte de la obligación de pagar si no quieres perder toda esta información.
- **De bloqueo**. Este tipo, en cambio, sí paraliza las funciones principales del equipo, como impedir el acceso al escritorio, restringir el uso del ratón, del teclado… Solo te permitirá interactuar con la ventana en la que exige el pago para volver a utilizar tu ordenador con total normalidad. Aunque bloquea el equipo, tus archivos personales no los suele modificar, por lo que están a salvo.

Las maneras que tiene el *ransomware* de infectar tu equipo

Estas son las vías más frecuentes que usan los y las ciberdelincuentes:

- **Aprovechar las vulnerabilidades** que puede ofrecer tu equipo, como un servidor web que no está actualizado o un sistema que no cuenta con los suficientes sistemas de seguridad.
- **Engañar a las personas usuarias** para que instalen el *malware* mediante un correo electrónico falso con un archivo adjunto, a través de un enlace, etc.
- ***Drive-by download***. Dicho con otras palabras, la descarga voluntaria o involuntaria de programas informáticos dañinos procedentes de Internet sin conocer sus consecuencias. Habitualmente, los verás en páginas con mensajes emergentes del estilo «si quieres seguir navegando en esta web, descarga X programa» o «baja este *software* para visualizar este contenido». En ocasiones, esta descarga se realiza de forma automática (si no clicas en ella, no pasará nada y podrás borrarla).
- ***Malwertising***. Se trata de incrustar anuncios maliciosos que contienen estas amenazas en páginas web aparentemente legales. La publicidad tiene un código que infecta el sistema de la persona usuaria sin que esta haga clic en él.

¿Qué debes hacer si tu ordenador se ve afectado por *ransomware*?

Lo primero es mantener la tranquilidad y seguir estas dos recomendaciones: **no pagar el rescate nunca** y, si no tienes un plan de respuesta para esta clase de incidentes, **utilizar la última copia de seguridad que tengas de tu información**. De este modo, recuperarás lo que hayas podido perder tras sufrir el ataque o, al menos, la mayor parte.

Te recomendamos no pagar, ya que al estar tratando con personas delincuentes, **nadie te asegura que lograrás la recuperación de tus archivos si pagas**. Además, si lo haces, cabe la posibilidad de que vuelvan a atacarte porque tienen la seguridad de que pagarás por ello.

Estos son los pasos a seguir en estos casos:

- **Contacta con el Centro de Respuesta a Incidentes de Seguridad e Industria** (CERTSI) del Instituto Nacional de Ciberseguridad (INCIBE). Te ayudarán a resolver este incidente, te explicarán cómo debes actuar y te ofrecerán información valiosa para que intentes recuperar tus archivos.
- **Desconecta el equipo** que esté infectado por este *malware* de la red. Así no seguirá atacando más documentos ni dispositivos ni se expandirá más.
- **Contacta con alguna persona técnica experimentada para que clone tu disco duro**. Además de ser de gran utilidad si quieres denunciar el ataque recibido, te servirá de gran ayuda para la **recuperación de los archivos** afectados. **Contar con sus servicios resulta a veces fundamental** en estos casos.
- **Denuncia el incidente** a la Guardia Civil o a la Policía Nacional. Ambos cuerpos cuentan con grupos especializados en estos ataques cibernéticos.
- Si puedes, **cambia todas las contraseñas** que hayas estado utilizando en la red. Una vez eliminado el ***ransomware*** vuelve a hacer este proceso.
- Procura **revisar que los demás servicios** de tu sistema funcionan correctamente.

¿Cómo puedes protegerte ante el *ransomware*?

Proteger a tu equipo de este tipo de *malware* es posible si adaptas una serie de medidas preventivas. ¡Toma nota!

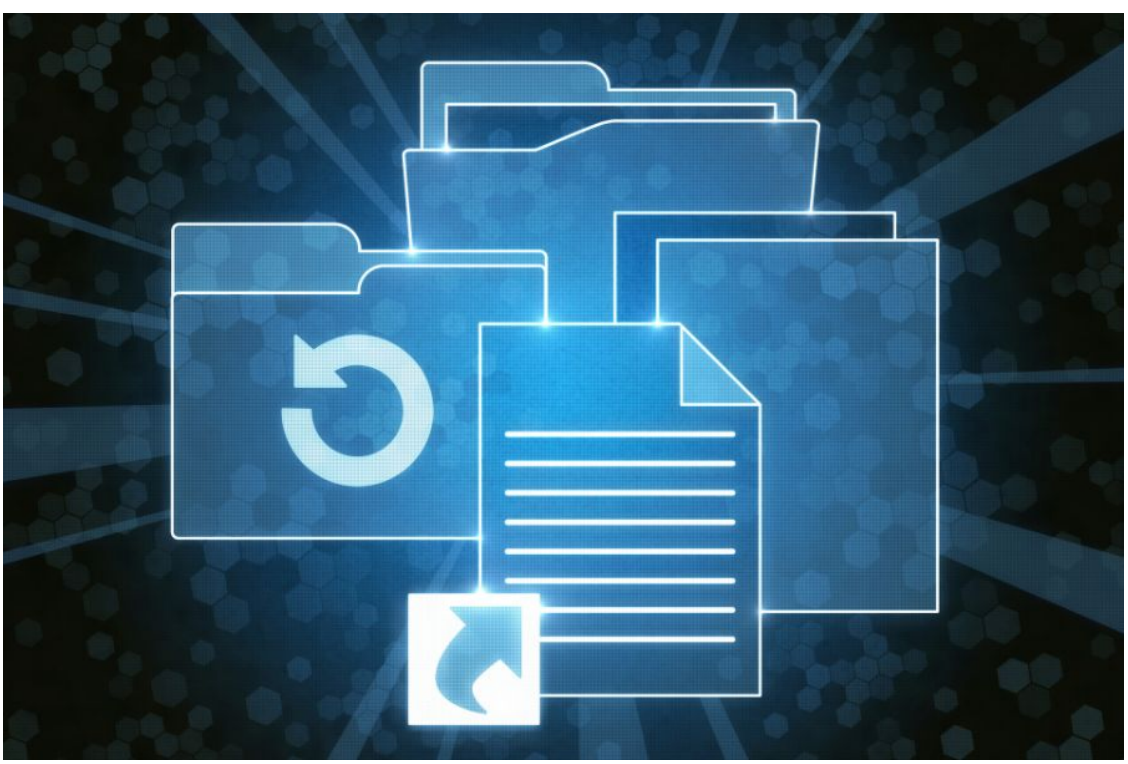
Las copias de seguridad

Si recibes un ataque de ***ransomware***, puede ser que la única medida que te permita recuperar tu información bloqueada sea **realizar copias de seguridad**.

Lo recomendable es que tengas, al menos, **dos copias actualizadas** y que, además, las tengas guardadas en un lugar diferente de tu dispositivo, como por ejemplo, en un disco duro externo. De esta manera, el *software* malicioso no podrá acceder a estos datos.

Realiza actualizaciones

Asegúrate que los sistemas operativos, dispositivos y aplicaciones que utilizas tengan habilitada la opción de **actualizarse automáticamente**, ya que los y las ciberdelincuentes aprovechan las vulnerabilidades de los mismos para poder entrar en el sistema. Si no sabes hacerlo, solicita ayuda a quien sepa hacerlo (amistades, familiares, etc.) o contacta con el soporte técnico correspondiente para que te faciliten esta puesta a punto.



Evita la exposición de tu red

Un cortafuegos es una gran opción para evitar que tu red quede expuesta a posibles ataques. Se trata de un sistema de seguridad que es capaz de establecer una serie de reglas para permitir o bloquear conexiones de entrada o salida a tu ordenador. Sistemas como Windows 10 ya vienen con estos cortafuegos instalados.

De esta manera, tu red estará más protegida de posibles ataques y, además, el propio ***firewall* o cortafuegos** te avisará de la intrusión de posibles amenazas.

Navega de forma segura

No entres en sitios web que sean de contenido dudoso. Hay algunas páginas que aparentan ser legítimas, pero lo que hacen es detectar las vulnerabilidades de tu sistema para introducir en él algún tipo de amenaza. Para poder evitar esto, es necesario tener actualizado el navegador web que uses y, sobre todo, que seas prudente en las actividades *online* que vayas a realizar:

- No abrir archivos adjuntos sospechosos que vienen en algunos correos con una dirección que no conoces.
- No pinchar en enlaces de páginas que no sepas hacia dónde te dirigen.
- No descargar contenidos ilegales de ninguna web.

Todas estas acciones reducen la posibilidad de que tu equipo se infecte.

Configura el correo electrónico adecuadamente

Una de las principales vías de entrada de toda clase de virus informáticos es el correo electrónico. Por ello, te recomendamos tomar ciertas medidas de seguridad:

- **Cuenta con filtros de *spam*** (correos electrónicos comerciales que te envían empresas o personas que desconoces). Estos filtros utilizan listas predefinidas con direcciones de correo no deseadas. Cuando veas que el filtro marca como *spam* alguna dirección que tú conoces y sabes que no es peligrosa, márcala como "no *spam*", y viceversa.
- **Emplea tu antivirus para escanear los correos electrónicos** que recibas. La mayoría los analizan automáticamente, pero asegúrate de que tiene habilitada esta opción entrando en los ajustes del antivirus.
- Si a pesar del escaneo y los filtros de *spam* te llega algún tipo de correo electrónico de dirección desconocida que salta estas dos barreras, **sé precavido** o **precavida**. Lo más aconsejable es no abrirlo y eliminarlo lo antes posible para evitar problemas.

Cuenta con un rápido plan de respuesta

Cuando ocurre algo de esto, es lógico ponerse nervioso o nerviosa y no tener claras las acciones a realizar. Si cuentas con un **plan de respuesta pensado previamente**, darás los pasos adecuados para eliminar el virus de tu sistema.

Ten claro con quién contactar para que te ayude en caso de que tu dispositivo se vea infectado y los pasos a realizar que ya hemos mencionado anteriormente (cortar la conexión, clonar el disco duro, denunciar el incidente, etc.).

Si cuentas con este plan, sabes mantener la calma y lo llevas a cabo paso a paso, tendrás mucho ganado. Es posible que tu ordenador nunca sea atacado, pero en el caso de que ocurra, te aseguramos que así será bastante más efectivo tomar cartas en el asunto.En definitiva, si eres precavido y cuentas con las medidas de seguridad necesarias, tu equipo está protegido del ***ransomware***. En el caso de que te ocurra, mantén la calma y sigue las instrucciones que te hemos ofrecido para resolver el problema y recuperar todos tus archivos..

vuela

4.5

Cómo proteger tu ordenador de un ataque de virus informático

En materia de ciberseguridad, algunas de las preguntas más frecuentes que se hacen las personas usuarias de un **ordenador** es **¿mi PC estará infectado por algún tipo de virus informático? ¿Cómo puedo saberlo?** ¿Qué tengo que hacer si lo está? Es una preocupación lógica, ya que nadie desea verse en esta situación. Sin embargo, dispones de una serie de pistas que te indicarán que tu dispositivo está en problemas.

En este apartado veremos la forma de detectarlo y, si lo está, los pasos que te recomendamos seguir para que todo vuelva a funcionar con normalidad.

Junta de Andalucía

Agencia Digital de Andalucía

¿Cómo puedes detectar que tu dispositivo está infectado?

Aunque la mayoría de las amenazas que existen hoy en día intentan pasar desapercibidas, hay varias **señales** que te ayudarán a identificarlas y combatirlas. Los principales **síntomas de que el dispositivo está infectado** son los siguientes:

- **Tu ordenador funciona especialmente lento**. Aunque existen distintas razones para que esto ocurra, como tenerlo demasiado tiempo en funcionamiento, disponer de muy poco espacio en el disco duro o emplear un programa demasiado potente para su capacidad, entre otros, es uno de los indicios que te pueden alertar de que un **virus** ha entrado en tu dispositivo.
- **Hay aplicaciones que no funcionan**. Si intentas arrancar aplicaciones que sueles abrir con total normalidad y estas no funcionan, es otro de los síntomas de una posible infección.
- **La temperatura del ordenador**. Una excesiva elevación del calor interno de tu PC puede deberse a que algún tipo de programa con intenciones maliciosas (*malware*) haya entrado en él. Su único objetivo será realizar acciones dañinas para tu dispositivo, tanto a nivel físico de sus componentes (estropeándolos por el aumento de temperatura) como de la información que guardas en su interior que puedan sustraerte.
- **Que la página de inicio de tu navegador cambie sola**. A veces, la infección provoca este cambio para reconducirte a páginas que suelen provocar otra serie de infecciones.

- **Tu antivirus ha desaparecido o está desactivado**. Cuando se introducen en tu dispositivo, algunas de estas amenazas están diseñadas para deshabilitar por completo tu antivirus para que, de esta manera, le sea imposible detectarlas.
- **En el momento de conectarte a Internet, se abren una serie de ventanas**. Este es un signo inequívoco de que **tu PC está infectado**, ya que existen amenazas que hacen esto para redirigir el tráfico hacia el lugar que a ellas les interesa.
- **No puedes conectarte a Internet**. Te es imposible acceder a la red o, si consigues hacerlo después de intentarlo varias veces, navegas muy lentamente. El *malware* que se haya infiltrado en tu dispositivo puede estar provocando esta situación, robando tu ancho de banda (la velocidad máxima a la que navegas con tu conexión a Internet).
- **Observas que el idioma de tu ordenador cambia**. Si tú no has sido quien que lo ha hecho, está muy claro que hay algo externo, como un virus, que ha querido configurarlo de esa manera.

Pasos a seguir en el caso de que descubras que tu dispositivo ha sido infectado

Si detectas que cualquier tipo de *malware* ha entrado en tu **ordenador**, no te pongas nervioso o nerviosa. Basta con que sigas una serie de sencillos pasos que te ayudarán a eliminar el **virus** de tu dispositivo por completo.

1. Corta tu conexión a Internet

El programa malicioso se suele alojar en tu memoria RAM, que es la que se encarga de almacenar de forma temporal los datos de las aplicaciones que estás usando para que funcionen, y de ahí pasa a infectar otra serie de archivos. Lo más conveniente es apagar la conexión WiFi o desconectar el cable del módem para aislar tu PC. Por ejemplo, **el *spyware* es un tipo de *malware* malicioso** que sigue tus actividades en línea mientras roba tu información, por eso es tan importante cortar el acceso a la red inmediatamente.

2. No ejecutes ningún programa

Si lo haces, cualquier tipo de archivo que tengas en él puede quedar **infectado** y, por lo tanto, perderás toda la información que contenga. Es mejor no utilizar ningún programa hasta haber eliminado la amenaza por completo.

3. Reinicia tu ordenador en modo seguro

Para hacerlo sigue estos sencillos pasos: apaga el ordenador, vuelve a encenderlo y cuando lo esté haciendo, pulsa F8 y haz clic en "Modo seguro con funciones de red".

En este modo y desconectado de Internet, tu dispositivo estará más protegido de la amenaza.

4. Elimina los archivos temporales

Algunos de estos programas maliciosos se inician al arrancar el PC. Si eliminas los archivos temporales de tu sistema, lograrás eliminarlos también a ellos. Para hacerlo, escribe en la barra del buscador de "Inicio" de Windows: "Liberador de espacio en disco". Una vez dentro, marca "Archivos temporales" en la lista de "Archivos que se pueden eliminar" y bórralos.

5. Realiza un análisis y escaneo del sistema

Si el sistema operativo de tu **ordenador** es Windows 10, este incluye una función que te permitirá analizar y **escanear** su contenido. Lo puedes hacer con la aplicación de seguridad **Windows Defender**. De esta manera, conseguirás detectar los programas de *malware* que haya en tu sistema.

Si prefieres hacerlo de forma manual, abre el menú "Inicio" y escribe "Seguridad". Luego, haz clic en "Seguridad de Windows". Una vez dados estos pasos pincha en "Protección antivirus y contra amenazas". Por último, haz clic en "Examen rápido". Se ejecutará un análisis completo del sistema y si encuentra algún tipo de *malware* te ofrecerá la posibilidad de **eliminar los archivos infectados inmediatamente de tu ordenador**.

Si tu sistema operativo no es Windows 10, te recomendamos utilizar un antivirus. Hay varios de ellos que tienen una versión gratuita que podrás obtener entrando en sus respectivas páginas webs. Los más destacados son: **Kaspersky** o **Avast**.

6. Reinicia el ordenador

Tras haber eliminado el motivo de la infección, reinicia tu PC. Ya no es necesario el modo seguro, por lo que puedes reiniciarlo con total normalidad.

7. Cambia tus contraseñas

Para proteger a tu equipo contra nuevos ataques, cambia todas las contraseñas que hayas empleado con anterioridad, ya que puede ser que el **virus** haya tenido acceso a ellas durante algún tiempo.

¿Cómo mantenerte protegido de los virus informáticos?

Ya estás en el punto en el que has conseguido eliminar el *software* malicioso o bien has tenido la suerte de no padecerlo todavía. Sea cual sea tu caso, este es el mejor momento para aplicar una serie de consejos y blindar tu ordenador ante cualquier amenaza.

Utiliza un antivirus

Aunque tu sistema operativo sea Windows 10, que ya trae su propia aplicación de seguridad, nuestra recomendación es que utilices un antivirus o ***software* de detección de *malware***. Parece algo muy evidente, pero es necesario mencionarlo, ya que es el primer paso para que en tu dispositivo no pueda entrar ningún tipo de *malware* y, si lo hace, sea detectado al instante y eliminado.

Ejecuta análisis programados con tu antivirus periódicamente

Configura el antivirus o el Windows Defender para que realice análisis periódicos. Lo aconsejable es que lo haga una vez por semana. Si necesitas usar el **ordenador** y te resulta molesto que se esté realizando este análisis a la vez, una buena opción es programarlo para que se ejecute cuando no lo estés empleando.

Protege tu red

Asegúrate de que tu conexión WiFi tiene una **protección adecuada** con cifrado WPA2 (te permite proteger las redes inalámbricas con contraseñas de hasta 63 caracteres). La mayoría de las compañías te ofrecen esta posibilidad. Para ello, escribe en tu navegador https://192.168.1.1 (o la que te facilite tu proveedor), introduce tus credenciales y accede al apartado de seguridad para activarlo.

Piensa antes de hacer clic

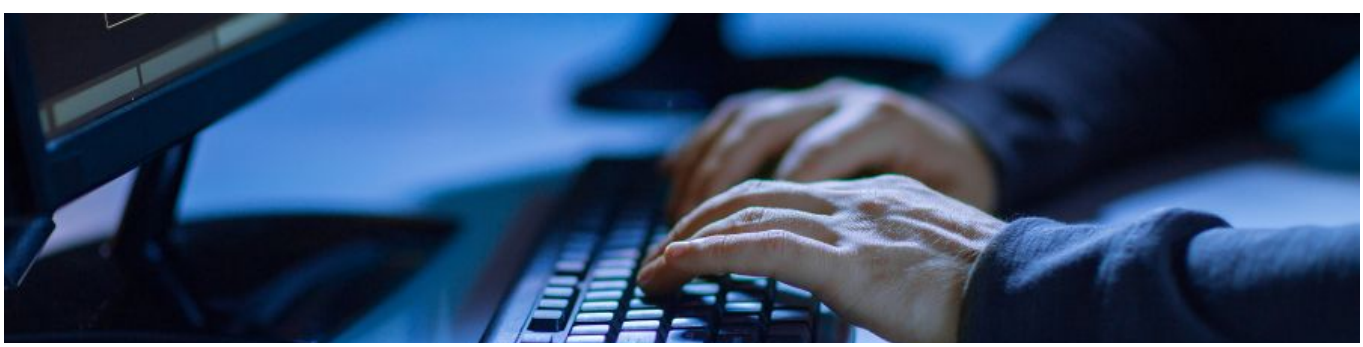
No abras archivos adjuntos que vengan en correos electrónicos que no conozcas, ni entres en sitios web que no sean de confianza ni pinches en archivos que no tienes muy claro a dónde te conducen. Resumiendo, **no hagas clic sin saber si lo estás haciendo de forma segura** y sin tener claro a qué página te diriges.

Mantén tu información personal segura

Aunque tu PC esté bien protegido, a veces expones tu información personal sin darte cuenta. Procura ser precavido a la hora de ofrecer este tipo de información en redes sociales o en cualquier página en la que se requiera un registro. **Configura bien la privacidad de tus redes sociales** para que solo las personas de tu confianza vean tu información y, si no es necesario, evita exponer información privada.

Realiza una copia de seguridad de tus archivos

Lo ideal es que tengas una copia de seguridad de todos los archivos que tengas en tu dispositivo. Si puedes, haz ese duplicado en un disco externo, ya que si hay algún tipo de problema en tu **ordenador**, tendrás todos tus archivos a salvo.Como has observado, existen una serie de pistas que te van a indicar si tu PC ha sido **infectado**. Sin embargo, si realizas los pasos que hemos detallado con anterioridad, tendrás la capacidad de detectar la amenaza y eliminarla. En cualquier caso, lo mejor es prevenir y aplicar las medidas de protección adecuadas para que tu dispositivo no vuelva a infectarse por ningún tipo de **virus informático**.




vuela