GOBIERNO DE ARAGON

## Manual del taller

# “SEGURIDAD EN INTERNET”

# Presentación. Taller de “Seguridad en internet”

Desde el Departamento de Hacienda, Interior y Administración Pública, se promueve la realización de este taller, con el objetivo de acercar a los participantes al mundo TIC, enseñando a utilizar de forma segura y adecuada las gestiones que los participantes necesiten.

Este manual forma parte de los materiales de la formación presencial que se lleva a cabo en centros públicos o de uso público de diversas localidades de la Comunidad Autónoma de Aragón.

Parte del contenido del presente taller se ha basado en el Manual de experiencia senior en ciberseguridad[1] desarrollado por la empresa INICIBE[2] y la oficina de seguridad del internauta[3].




Última actualización de este manual: octubre 2024.

Talleres TIC [4]

Talleres TIC. Manuales; 23

GOBIERNO DE ARAGON

[1] https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
[2] https://www.incibe.es/
[3] https://www.incibe.es/ciudadania/
[4] https://www.aragon.es/-/talleres-tic

# Índice de contenidos

# 01. ¿Qué es la seguridad informática?

La seguridad informática es la rama de la informática que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

Para estar protegidos no necesitamos grandes conocimientos informáticos ni equipos avanzados, sólo se necesita sentido común y seguir paso a paso los consejos de esta guía.

## 1.1. Glosario sobre seguridad

Para empezar, vamos a definir algunos conceptos sobre seguridad:

### Ciberseguridad

Es la práctica de proteger los sistemas, dispositivos y redes de ataques digitales. Estos ataques buscan conseguir, acceder, modificar o destruir la información confidencial. Otros ataques pueden ir enfocados a la extorsión de los usuarios o a afectar el funcionamiento de un negocio o empresa.

### Seguridad informática

Es el área de la informática que pretende proteger en especial la información contenida en un ordenador, tableta o redes de ordenadores. Para que podamos conseguir esta protección existe una serie de reglas, protocolos y leyes diseñadas para reducir los riesgos a los que nos exponemos.

### Seguridad de la información

Se compone de una serie de medidas que permite a organizaciones resguardar, proteger y asegurar la integridad de la información y la confidencialidad y además asegurar la disponibilidad de los datos.

### Malware

Es un tipo de software, es decir, un programa o aplicación que pretende causar algún perjuicio en el dispositivo que se ha instalado o al usuario del dispositivo.

## 1.2. ¿Por qué es necesario protegerse?

Todos nosotros utilizamos dispositivos con acceso a internet, móviles, tabletas u ordenadores. Los utilizamos para muchas cosas, trabajar, jugar a juegos por internet, hablar con familiares… La mayoría de nosotros los usamos además para tomar fotografías, y realizar compras por internet.

Todo esto hace que nuestros dispositivos contengan una gran cantidad de información sensible, por eso es tan importante aprender a protegernos de personas con malas intenciones o personas que quieran acceder a nuestro contenido sin autorización.

### ¿Cómo saber si estamos protegidos?

La mayoría de dispositivos ya cuentan con herramientas de protección contra diferentes amenazas. El antivirus es nuestra principal protección contra ellas y es el mejor filtro que podemos tener para detectar y eliminar cualquier tipo de virus o malware.

Vamos a ver cómo podemos saber si estamos protegidos en diferentes sistemas:

Windows 10

Este sistema operativo tiene varias opciones de seguridad preinstaladas:

1. Hacemos clic en el icono de Windows y seleccionamos la rueda de configuración.

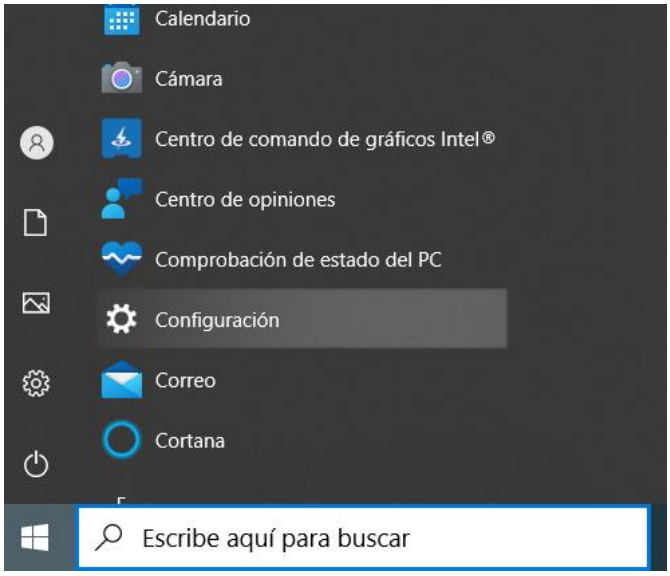


Imagen 1: Menú configuración Windows

2. Seleccionamos el apartado “actualización y seguridad”.


Imagen 2: Pantalla menú configuración de Windows 10

3. Aparece la opción “seguridad de Windows”.


Imagen 3: Menú de Seguridad Windows 10

4. Aquí vemos las distintas áreas de protección disponibles, si todo está bien estarán marcadas con un check verde. Dentro de la opción “Protección contra virus y amenazas” Podemos ver si las opciones de protección se encuentran activadas y configuradas o incluso hacer un examen rápido para asegurar que nuestro equipo está libre de virus.

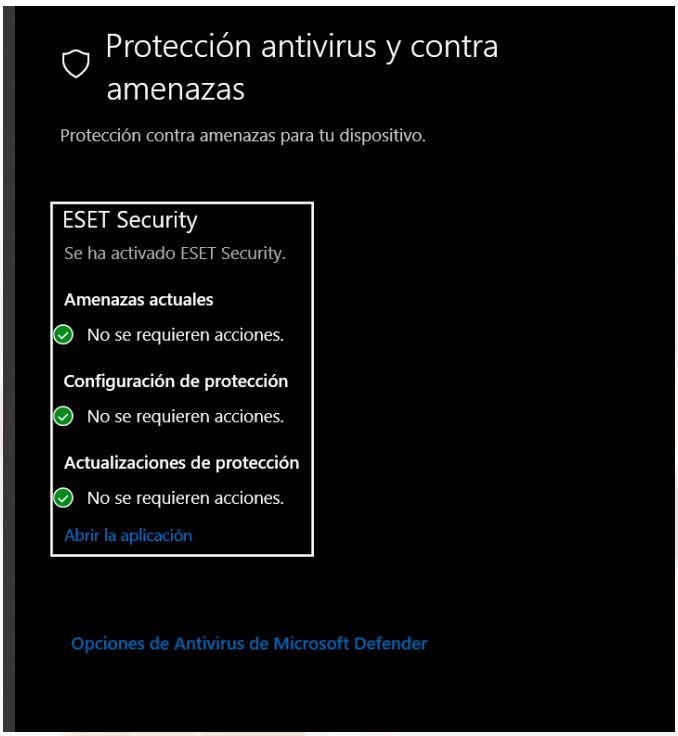


Imagen 4: Menú protección contra virus y amenazas

En Android

En los dispositivos Android existe una herramienta llamada Google play protect que nos sirve para protegernos de amenazas. Vamos a comprobar si se encuentra activada:

1. Accedemos a la aplicación Play Store y pulsamos sobre el icono de nuestra cuenta en la esquina superior derecha.

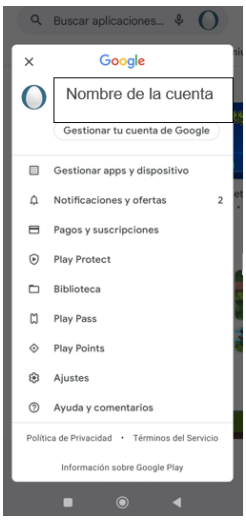


Imagen 5: Menú configuración Play Store

2. Seleccionamos la opción Play protect, una vez dentro, veremos el estado general de nuestro dispositivo y la última vez que se realizó un análisis del mismo.

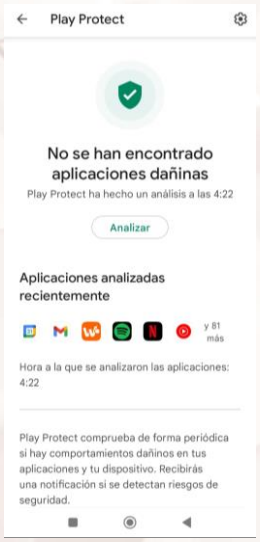


Imagen 6: Play Protect

3. Finalmente, para asegurar la máxima protección, en el menú de configuración podemos activar las opciones de “Analizar aplicaciones con Play Protect” y “Mejorar la detección de aplicaciones dañinas”.

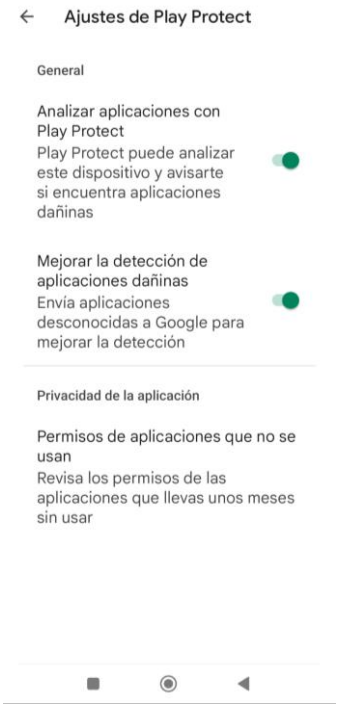


Imagen 7: Menú ajustes Play Protect

En MacOS

Los dispositivos Apple también disponen de herramientas de seguridad preinstaladas. Para comprobar si están activadas:

1. Vamos al “Menu apple” y en preferencias del sistema, buscamos el apartado de seguridad y privacidad y pulsamos en general.

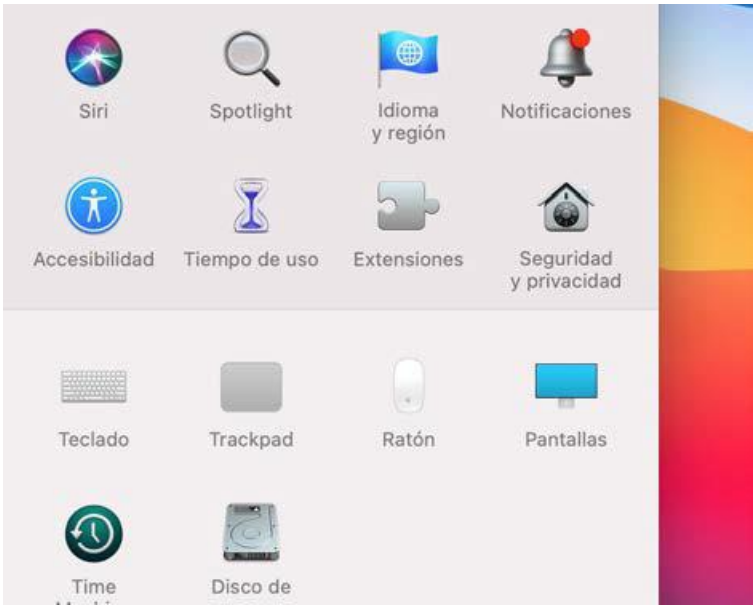


Imagen 8: Menú de Apple

2. En caso de que el menú se encuentre bloqueado apretamos en el candado y nos pedirá que nos identifiquemos.

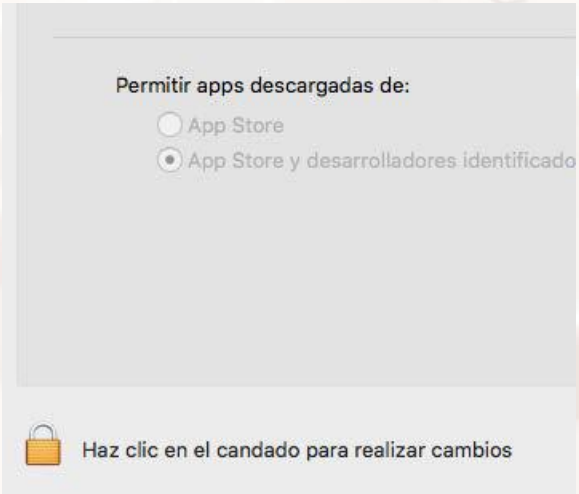


Imagen 9: Identificación en Apple

3. Una vez dentro, seleccionaremos las fuentes de las que permitiremos que se instalen las aplicaciones y marcaremos únicamente el “apple store”. Es la opción más segura porque todas las aplicaciones tienen que pasar por filtros de seguridad estrictos.

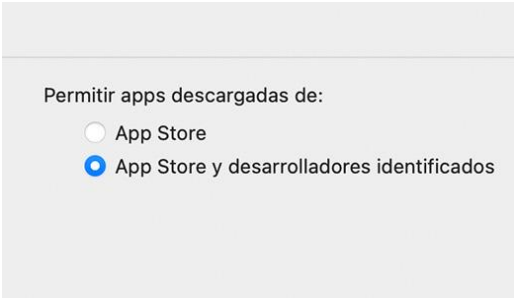


Imagen 10: Menú de orígenes de aplicaciones.

En iOS

La protección principal de estos dispositivos son los filtros de seguridad de Apple Store, que se encuentran habilitados por defecto para todos los usuarios.

# 02. ¿Cuáles son los riesgos más comunes?

## 2.1 Fraudes y engaños

Como ya sabemos, internet puede ser un lugar lleno de ventajas y posibilidades si sabemos cómo navegar de forma segura, porque no sólo podemos sufrir ataques directos de otras personas a nuestros dispositivos para obtener información o archivos que tengamos guardados, sino que también podemos encontrarnos fraudes o engaños que intenten hacer que demos nuestra información de forma voluntaria.

Por eso es importante conocer cómo funcionan los fraudes y estafas más comunes de la red para luego poder estar prevenidos y evitarlos. Solo necesitaremos utilizar el sentido común y estar atentos, pues muchos de estos fraudes se aprovechan de la información que recaban sobre nosotros para lanzar ataques dirigidos basados en nuestros intereses, nuestra situación actual o se hacen pasar por personas o servicios de confianza. Por suerte, su modus operandi suele ser el mismo y, una vez sepamos cómo funcionan, podremos identificarlos y prevenirlos rápidamente.

### Falsos chollos

Cuando compramos por internet hay que estar siempre alerta, porque sin darnos cuenta podemos terminar en una tienda fraudulenta o realizando un trato con un vendedor con malas intenciones. Para evitarlo os damos una serie de consejos y buenas prácticas:

1. Comprobar la URL: Este debe ser siempre nuestro primer paso, aunque no es un método completamente fiable, pero nos ayudará a descartar tiendas online que no utilicen una conexión segura (es segura si la URL comienza con ‘https://’) y sean un riesgo a nuestra seguridad.

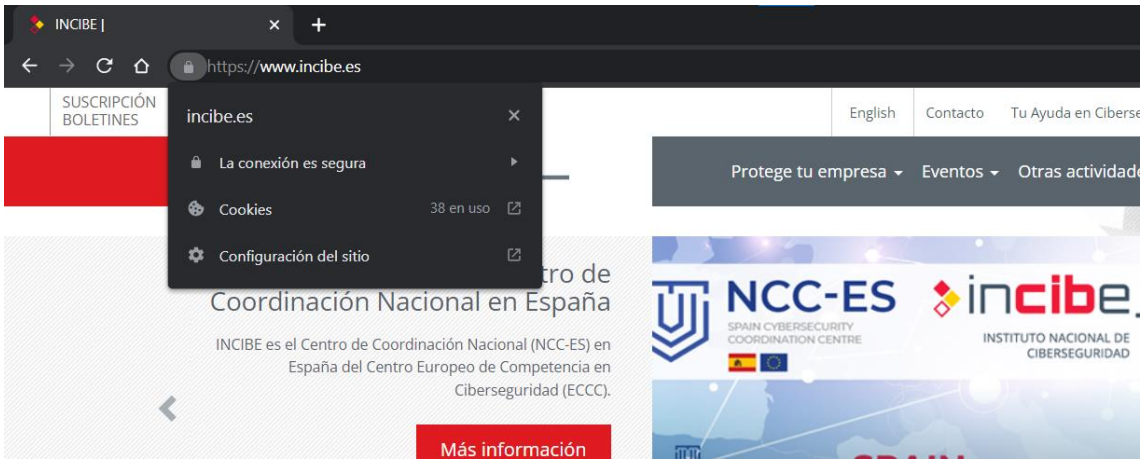


Imagen 11: Dirección web segura

2. Al revisar la dirección web también veremos si coincide con el nombre de la empresa o tienda. Así evitaremos entrar en webs falsas o que suplantan a una marca conocida.

3. Buscar información de la empresa: una tienda online legítima dispondrá de un apartado con información sobre la empresa, NIF y otros datos. Es común que se encuentre dentro de un apartado llamado Aviso legal, Contacto o Información.

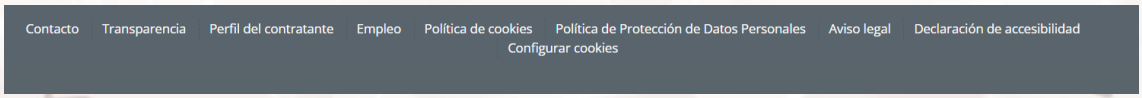


Imagen 12: Muestra de contacto y aviso legal

4. Buscar un sello de confianza: son acreditaciones que tienen como objetivo demostrar al usuario que se trata de un negocio legítimo, preocupados por la seguridad y el bienestar de los consumidores. Por norma general, se encuentran en la parte inferior de la tienda online, en forma de logotipo.


Imagen 13 Ejemplos de sellos de confianza

5. Los métodos de devolución de los productos nos pueden dar información sobre si la página web es fraudulenta o no. Por lo general en las webs falsas la información sobre la devolución de productos no aparece o es muy escasa.

6. El precio de los productos es otro indicador. Es normal que las páginas web tengan descuentos o promociones, pero los precios muy bajos deben hacernos sospechar.

7. Examinar la valoración de otros usuarios: es recomendable realizar búsquedas sobre la opinión y comentarios de otros usuarios. En el caso de que no encontremos las valoraciones o que todas sean muy buenas y parezcan hechas por un robot, deberemos desconfiar. Lo normal en una tienda online es que haya comentarios tanto positivos como negativos y muy variados.

8. Comprobar la reputación: si es una tienda o un vendedor online, revisar su reputación u opiniones de otros usuarios en Internet puede ayudarnos a evitar una estafa, incluso si la web está llena de comentarios positivos.

## Métodos de pago seguros

Otro punto que debemos tener presente para evitar engaños es el método de pago, existen métodos de pago más seguros que otros, para eso tenemos que conocer los métodos menos seguros y así poder identificarlos.

- PayPal[5]: Es un medio bastante extendido para realizar pagos por internet, por su versatilidad y sencillez a la hora de usarlos. Es una referencia en el mundo de los pagos por internet. Además, su sistema de devoluciones es sencillo lo que lo hace un medio muy útil para compradores habituales.

- Tarjeta bancaria: Es la manera más sencilla de comprar online a través de un sistema similar al que usaríamos para pagar en una tienda física. Es quizá el método más cómodo para los compradores esporádicos. En el mercado actual, parece la opción más razonable en cuanto al equilibrio de facilidad de integración, costes, seguridad de la transacción etc…

- Contra reembolso: Es un método que está prácticamente en desuso, en el que el propio repartidor cobra al cliente en el momento de la entrega. Aunque la integración es inexistente requiere de repartidores o empresas logísticas con equipamiento y autorización para gestionar y mover el dinero.

- Transferencias bancarias: Son un método poco recomendable, las experiencias con ellas suelen ser malas, nos obligan a transferir el dinero a un número de cuenta sin tener prueba de compra.

- Pago a través del móvil: Es cómodo rápido y funcional, pero su penetración en el mercado aún no es suficiente como para ser una carta a la que jugarse el todo por el todo.

[5] https://www.paypal.com/es/home

- Bancos online: Cada vez hay más, se trata de una buena opción para los clientes que utilizan este tipo de banca pero, de nuevo, parece que no hay una base suficiente aún como para soportar grandes bases de clientes.

- Tarjetas almacenadas en grandes plataformas: Google, Amazon, Apple disponen de los sistemas necesarios para poder almacenar tarjetas bancarias. Esto los convierte en potenciales medios de pago y, como es habitual en ellos, están intentando extenderse en este mercado también.

Estos son algunos métodos de pago extendidos, por lo general las transferencias bancarias a bancos extranjeros son uno de los métodos favoritos de los ciberdelincuentes, mientras que las plataformas de pago seguro, el contrarrembolso o el pago mediante tarjetas de crédito suelen ser típicos de negocios legítimos.

Es fundamental que a la hora de comunicarnos con las tiendas lo hagamos mediante las plataformas oficiales y a la hora de pagar usemos las herramientas de pago habilitadas.

## Otro tipo de fraudes y engaños

Otros tipos de engaños y fraudes que pueden aparecer son:

- Préstamos engañosos: es habitual encontrar anuncios o publicaciones en redes sociales de personas que se ofrecen a conceder préstamos a un muy bajo interés porque quieren ayudar a las personas. Este tipo de anuncios requiere que realicemos algún pago inicial a modo de gastos administrativos o bajo cualquier premisa, para que luego esta persona desaparezca.

- Webs falsas: las webs falsas copian el estilo de otras webs más famosas o de marcas conocidas, utilizando sus colores, logos y estructura. Sin embargo, pueden encontrarse diferencias si nos fijamos bien, como imágenes de menos calidad, falta de información sobre la empresa o una URL sin HTTPS y sin certificado de seguridad.

- Concursos falsos: si hemos ganado un sorteo sin haber ni siquiera participado, lo más probable es que sea un fraude. Otros concursos utilizan formularios de registro donde nos piden demasiados datos personales (número de tarjeta, email, DNI…) o compartirlos con todos nuestros contactos para llegar a más víctimas.

- Suscripciones Premium de SMS: algunos servicios utilizan los SMS como método para financiarse, al cobrar por cada SMS que enviamos. Sin embargo, algunos fraudes utilizan este medio sin nuestro consentimiento, al descargarnos alguna app fraudulenta o al responder a un SMS sospechoso, por eso debemos tener mucho cuidado y estar alerta en este tipo de comunicaciones.

- Sextorsión: en el caso de que hayamos conocido a alguien por Internet y esta persona nos solicite pasar al segundo nivel al compartir fotografías o vídeos íntimos debemos desconfiar, después podrá utilizar ese material para chantajearnos.

## 2.2. Ingeniería social

La ingeniería social son un conjunto de técnicas empleadas para conseguir datos de usuarios de servicios o páginas web. Existen distintos tipos de ataques basados en el engaño y la manipulación, aunque sus consecuencias pueden variar mucho. Este tipo de técnicas se suele utilizar como paso previo a otros ataques.

Por lo general el objetivo de este tipo de ataques es obtener datos personales y/o bancarios de los usuarios, haciéndonos creer que los estamos compartiendo con alguien de confianza.

También pueden utilizar esta técnica para que descarguemos malware con el que infectar y/o tomar control del dispositivo.

## Pishing

Consiste en el envío de un correo electrónico donde los ciberdelincuentes suplantan la identidad de entidades de confianza, como nuestro banco, una red social o una entidad pública para obtener toda la información personal y bancaria que puedan. También es común que adjunten archivos infectados o enlaces a páginas fraudulentas.

## Vishing

Consiste en la realización de llamadas telefónicas haciéndose pasar por entidades de confianza, como nuestro banco o un servicio técnico para engañar a los usuarios, obteniendo sus datos personales o tomando control de sus dispositivos.

## Smishing

Consiste en el envío de mensajes de texto (SMS) o por aplicaciones de mensajería instantánea, haciéndose pasar por entidades de confianza o contactos de la víctima para obtener información personal y bancaria.

## Spam

Consiste en el envío de grandes cantidades de mensajes o envíos publicitarios a través de Internet sin haber sido solicitados, es decir, se trata de mensajes no deseados. La mayoría tienen una finalidad comercial, aunque puede haberlos que contengan algún tipo de malware.

## ¿Cómo identificar ataques de ingeniería social?

Para identificarlos, lo primero es no dejarnos llevar por la presión y utilizar el sentido común, este tipo de ataques intenta hacer que actuemos en el momento y evitar que pensemos con lógica.

Como los tres tipos de ataque comparten una forma de contacto inicial similar, podemos crear una serie de pasos a seguir que nos valgan para identificar todos ellos, aunque en nuestro caso nos vamos a centrar en el phishing:

1. **Comprobar el remitente** (phishing, smishing y vishing): Es el primer paso y el más evidente. Comprobamos si la dirección de correo o el número de teléfono que nos contacta es conocido. Sospecharemos cuando:

    - No sea alguien con quien mantengamos contacto de forma habitual.

    - Conozcamos al remitente, pero el contenido es diferente al habitual.

    - La dirección desde la que nos escribe es rara, es decir, no coincide exactamente con la dirección oficial que conozco.

2. **Analizar el asunto** (phishing): La mayoría de fraudes utilizarán un asunto llamativo que capte nuestra atención para que ignoremos el resto de alertas. Puede empezar por palabras como “AVISO”, “URGENTE” o “IMPORTANTE”. También tenemos que estar especialmente atentos cuando el asunto empieza por “Re:” Esto significa que es la respuesta a un correo anterior relativo al asunto expuesto, pero lo más probable es que nunca hayamos enviado un correo a esa cuenta.

3. **Analizar el objetivo del mensaje** (phishing, smishing y vishing): Debemos preguntarnos qué quieren de nosotros. Si es una entidad como nuestro banco, lo más probable es que ya tenga nuestros datos y no necesite volver a pedírnoslos. Estos mensajes suelen solicitar llevar a cabo una acción de manera urgente, para evitar que nos paremos a analizar el mensaje, por ello es probable que se trate de un fraude.

4. **Examinar la redacción** (phishing y smishing): Los errores ortográficos y gramaticales son típicos de mensajes escritos con prisas o mediante una traducción automática, lo que debe hacernos sospechar.

5. **Comprobar los enlaces** (phishing y smishing): si el mensaje incluye un enlace, debemos comprobar si es fiable o no pasando el cursor por encima o manteniendo el dedo sobre el mismo y comprobar cuál es la URL real.

   **NOTA:** Es importante no abrir el enlace de ninguna manera si tenemos algún tipo de duda.

6. **Analizar el adjunto** (phishing y smishing): Antes de descargar ningún adjunto, deberemos analizarlo con nuestro antivirus para asegurarnos de que no se trata de un malware. Finalmente, debemos recordar qué si sospechamos de un fraude, nunca debemos seguir sus indicaciones, ni facilitar ningún tipo de información personal.

## 2.3. Noticias falsas

Las fake news son noticias falsas y bulos que se propagan por la Red con el único objetivo de desinformar, engañar y manipular a los usuarios. Gracias a su capacidad de difusión a través de las redes sociales y las aplicaciones de mensajería instantánea, como WhatsApp, se han convertido en un verdadero problema, ya que llegan a nosotros antes que las noticias reales.

### ¿Cómo identificarlas?

Para identificar las noticias falsas podemos seguir una serie de consejos:

1. Buscar la fuente y contrastar la noticia: las noticias reales siempre mencionarán las fuentes utilizadas, que podremos utilizar para contrastar la noticia.

2. Revisar la URL: es frecuente que las noticias falsas se alojen en webs falsas o poco fiables que no dispongan de certificado de seguridad ni HTTPS en la URL.

3. Mirar más allá del titular: suelen recurrir a titulares muy llamativos, agresivos o sensacionalistas. Su objetivo es apelar a nuestras

emociones, aunque un rápido vistazo a la noticia nos ayudará a desenmascarar el fraude.

4. Comprobar el formato: las noticias falsas no suelen cuidar el formato, utilizan imágenes de poca calidad, manipuladas y presentan faltas de ortografía.

5. Aplicar el sentido común: no debemos dejarnos llevar por las emociones, si la noticia parece que busca atacar, manipularnos o dividir, debemos desconfiar.

### Contrastar fuentes

Para asegurarnos que la noticia es veraz se recomienda después de cumplir todos los pasos anteriores buscarla en más de un medio de comunicación oficial.

## 2.4. Tipos de amenazas

A parte de los que ya hemos visto existen diversas tácticas de las que se pueden aprovechar los ciberdelincuentes. Es necesario conocerlas para poder prevenir que las usen con nosotros, vamos a ver un poco sobre ellas.

### Ataques a contraseñas

Una de las tácticas más utilizadas es atacar directamente a las contraseñas de los usuarios. En general solemos ponerles las cosas fáciles porque por fuerza de hábito tendemos a utilizar las mismas contraseñas para varios servicios, utilizar información personal o incluso a apuntarlas en sitios vulnerables.

Existen diversos tipos de ataques a nuestras contraseñas dependiendo de cómo se realicen, los podemos clasificar:

- Ataque por fuerza bruta: Consiste en intentar adivinar la contraseña a partir de palabras y números aleatorios, dependiendo de la información personal que tengan de nosotros les será más sencillo “adivinar” nuestra contraseña.

- Ataque por diccionario: Mediante un programa va probando todas las palabras de un diccionario empezando por letras sencillas “a”, “AA”… Hasta dar con la combinación adecuada de letras, números y símbolos.

El objetivo más habitual de este tipo de ataque suelen ser nuestras cuentas de correo electrónico, porque eso les permite acceso a todas las cuentas de todas las páginas vinculadas a ese correo.

## Ataques por malware

Malware es cualquier pieza de software, es decir, programa que quiera realizar alguna acción dañina para nuestro dispositivo o para nosotros mismos. Dependiendo de la forma en la que actúen pueden ser de varios tipos:

- Virus: Están diseñados para copiarse a sí mismos y propagarse a tantos dispositivos como les sea posible, para eso lo hacen a través de aplicaciones, correo electrónico, memorias USB… Son capaces de dañar un sistema o modificar o eliminar archivos en el equipo.

- Troyanos: Los troyanos se camuflan como un software legítimo para infectar nuestro equipo, también pueden hacerlo a través de ataques de ingeniería social.

- Spyware: Es un tipo de malware que una vez instalado en un equipo comienza a recopilar información. Supervisa toda la actividad del dueño del dispositivo y comparte esta información con una tercera persona. También es capaz de descargar e instalar otros malware.

- “Apps” maliciosas: Las Apps maliciosas se hacen pasar por aplicaciones legítimas o tratan de emular a otras aplicaciones de éxito. Una vez instaladas en el dispositivo, nos pedirán una serie de permisos abusivos o, por el contrario, harán un uso fraudulento de dichos permisos.

Si queremos conocer en más profundidad a qué tipos de ataques nos podemos enfrentar podemos visitar la web del Instituto Nacional de Ciberseguridad.[6]

También podemos ver la guía de ciberseguridad para todos[7].

## 2.5. Actividad 1

Piensa en las actividades que realizas en tu día a día en internet, elabora una lista con ellas. Acorde a las amenazas que hemos visto hasta ahora en el curso elabora una lista de brechas de seguridad posibles.

Además puedes realizar el Test de ciberseguridad[8] y el Test de compras por internet[9].

[6] https://www.incibe.es/ciudadania/
[7] https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
[8] https://www.incibe.es/ciudadania/formacion/autoevaluacion
[9] https://www.incibe.es/ciudadania/formacion/autoevaluacion

# 03. Mecanismos de seguridad

Ahora que conocemos algunos de los tipos de ataques que podemos sufrir y de malware que puede afectarnos, vamos a aprender de qué forma nos podemos proteger contra ellos.

## 3.1. ¿Cómo proteger nuestra privacidad y nuestros datos?

La contraseña es la principal defensa que tenemos a la hora de proteger nuestros datos, pero debemos tener en cuenta ciertos factores a la hora de usarla y aplicarla.

### Uso de contraseñas

Lo primero que se nos pide a la hora de utilizar un nuevo dispositivo es establecer una contraseña, normalmente los nuevos dispositivos nos piden que los vinculemos a una cuenta de correo que nos permitirá añadir una capa extra de protección al dispositivo, además de poder crear una nueva contraseña en caso de olvidarnos de ella.

Para que nuestras contraseñas sean lo más efectivas posibles y minimizar riesgos se recomienda:

- Utilizar gestores de contraseñas. Son programas que se encargan de proteger e introducir nuestras contraseñas cuando son necesarias.
- No repetir la misma contraseña en distintas cuentas.
- Cambiar las contraseñas cada 3 meses.
- No compartirlas con nadie, ni amigos ni familiares.

## Creación de contraseñas robustas

Para crear contraseñas seguras se recomiendan los siguientes pasos:

1. Pensar una frase de 10 caracteres mínimo (un carácter es una letra, símbolo o número). Puede tener significado para nosotros o simplemente unir 2 o 3 palabras al azar, pero que nadie más conozca: Ejemplo: Mi cuenta segura.

2. Alternar mayúsculas y minúsculas. Unimos las palabras y resaltamos las iniciales con mayúsculas: Ejemplo: MiCuentaSegura.

3. Sustituir letras por números. Un truco es intercambiar algunas letras por cifras, como “o” por 0, “i” por 1, “e” por 3 o “a” por 4: Ejemplo: M1Cu3nt4S3gur4.

4. Incluir algún símbolo (~! @ # $% ^& * -+ = ‘ | \ \ ( ) { }\ [ ]:; “’ < >,.? /).: Ejemplo: M1Cu3nt4S3gur4!

5. Personalizar la clave para cada servicio. Podemos utilizar las dos primeras letras del servicio y una la ponemos al principio y otra al final de la clave, ambas en mayúsculas.  Ejemplo: si el servicio se llama “Mailbook”, usaremos la M y la A: MM1Cu3nt4S3gur4!A.

## Verificación en dos pasos

Es un mecanismo de protección adicional que tiene como objetivo evitar que alguien sin autorización pueda acceder a nuestras cuentas online.

Para eso a parte de la contraseña utiliza otra vía de confirmación de usuario, normalmente una clave o código enviado a través de otro medio, que puede ser un correo electrónico, un mensaje SMS a un teléfono móvil…

Esta clave o código será de un solo uso, sólo son válidos durante un tiempo limitado y deberemos introducirlo además de nuestra contraseña para verificar nuestra identidad.

Es recomendable activar la verificación en dos pasos porque así se añade una capa extra de protección a nuestras cuentas. La mayoría de las aplicaciones cuentan con la posibilidad de una verificación en dos pasos.

## Bloqueo de dispositivos

La mayoría de los dispositivos por defecto establecen un bloqueo de dispositivo, bien sea a través de un PIN, un patrón o clave de seguridad. Este bloqueo se puede activar de forma manual o se activa por defecto tras un tiempo de inactividad, para evitar que terceras personas puedan acceder a nuestro dispositivo de forma física.

Por lo general en dispositivos móviles existen varios tipos de bloqueo, los más comunes son:

- Patrón: consiste en un dibujo trazado, uniendo una serie de nueve puntos en forma de un cuadrado de 3x3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla, también se puede configurar para que no aparezca el trazo a la hora de dibujarlo.

- PIN: se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.

- Contraseña: se trata de una clave de al menos 4 dígitos y letras.

- Desbloqueo con huella dactilar: nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o tableta simplemente poniendo el dedo sobre el lector de la huella.

- Desbloqueo facial: nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.

- Desbloquear con dispositivo Bluetooth: podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o tableta, como una pulsera de actividad o reloj inteligente.

Cuando seleccionemos la opción que más nos convenga, se nos pedirá configurar un método extra de desbloqueo para poder utilizar el dispositivo en caso de que el primero falle.

## 3.2. Uso de antivirus para tu Smartphone

Al igual que en nuestros ordenadores el resto de dispositivos informáticos de los que disponemos (tabletas, móviles…) pueden ser vulnerables a ataques externos, para evitar que sean atacados o que estos ataques tengan éxito la mejor defensa que podemos tener es un antivirus.

### ¿Qué es un antivirus?

Un antivirus es un programa que nos permite detectar y eliminar virus informáticos (malware).

### Tipos de antivirus

Dependiendo de la función que tengan se pueden clasificar en:

- Preventores: Se caracterizan por avisar antes de que se presente la infección. Este tipo, por lo general, permanece en la memoria del computador, monitoreando las acciones y funciones del sistema.
- Identificadores: identifican programas infecciosos que pueden afectar el sistema. Además, rastrean secuencias de códigos específicos vinculados con dichos virus.
- Descontaminadores: Se especializan en eliminar programas malignos.

Actualmente los antivirus suelen tener características de todos los tipos anteriores, aunque se especialicen en alguna de ellas.

### Google play protect

Es un servicio de protección de dispositivos Android, normalmente viene preinstalado en estos dispositivos. Se dedica a analizar las aplicaciones que se

instalan en el dispositivo y nos avisa en caso de que algún software pida acceso a nuestro dispositivo.

Descarga e instalación

Como ya se ha dicho, se encuentra instalado por defecto en todos los dispositivos Android por encima de la versión 6.0. Podemos comprobar si está activo siguiendo los pasos recogidos en la sección 1.2 de este manual.

Tipo de protección

Este antivirus permite analizar de forma previa las aplicaciones antes de instalarlas, para prevenir posibles instalaciones de malware y además permite analizar y descontaminar nuestro dispositivo, ya que elimina aplicaciones o configuraciones que pueden ser dañinas para el dispositivo.

¿Qué puede llevar a cabo?

A continuación, se recogen algunas de las funciones que tiene este antivirus:

- Verifica la seguridad de las aplicaciones de Google Play Store antes de descargarlas.
- Analiza la actividad del dispositivo para detectar aplicaciones potencialmente dañinas de otras fuentes, conocidas como software malicioso.
- Nos advierte sobre aplicaciones potencialmente dañinas.
- Puede desactivar o quitar aplicaciones dañinas de tu dispositivo.
- Nos avisa sobre cualquier aplicación que infrinja la política de Software No Deseado[10] por ocultar información importante.
- Nos envía alertas de privacidad acerca de las aplicaciones que pueden obtener permisos de los usuarios para acceder a tu información personal.

[10] https://www.google.com/about/unwanted-software-policy.html

## AVG antivirus

AVG Technologies (anteriormente Grisoft) es una empresa privada de la República Checa especializada en software de seguridad y privacidad informática.

AVG es uno de los antivirus gratuitos mejor valorados, permite analizar nuestros dispositivos en tiempo real o incluso llevar a cabo análisis de los mismos.

Descarga e instalación

Para instalarlo en nuestro dispositivo, buscamos el antivirus en la aplicación de confianza para el mismo, ya sea play store[11] o apple store[12].

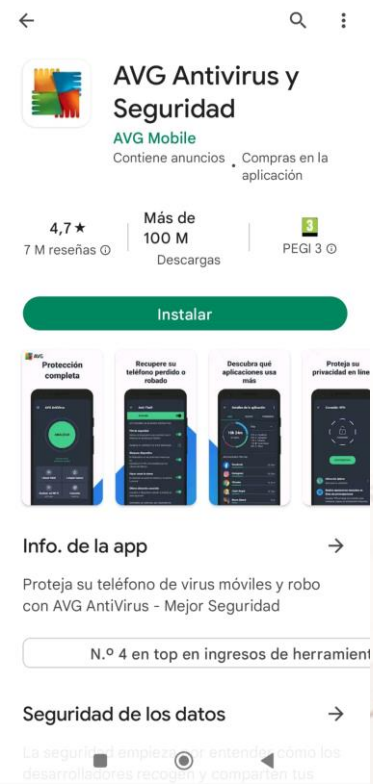


Imagen 14: AVG en Play Store

Apretamos en el botón de instalar, nos pedirá permisos de acceso a nuestro dispositivo para poder analizar y eliminar el malware que pueda encontrar.

[11] https://play.google.com/store/apps/details?id=com.antivirus
[12] https://apps.apple.com/es/app/avg-seguridad-y-privacidad/id1473934066

¿Qué puede llevar a cabo?

- Analizar aplicaciones, juegos, configuración y archivos en tiempo real.
- Detener tareas que ralentizan nuestro dispositivo para aumentar la velocidad.
- Limpiar archivos innecesarios para liberar espacio.
- Bloquear aplicaciones privadas con un PIN, patrón o huella dactilar.
- Localizar nuestro teléfono extraviado mediante Google Maps.
- Ocultar fotos privadas en un baúl cifrado.
- Mantener nuestro anonimato con una VPN.
- Analizar redes Wi-Fi en busca de amenazas.
- Detectar y bloquear los sitios de estafa para mejorar su seguridad.
- Verificar la velocidad de subida y bajada de la red Wi-Fi.
- Recibir alertas si nuestras contraseñas se filtran.
- Obtener información sobre el nivel de permisos de las aplicaciones instaladas.

## Kaspersky

Kaspersky Lab es una compañía internacional dedicada a la seguridad informática con presencia en aproximadamente 195 países del mundo. Su sede central se encuentra en Moscú, Rusia.

Kaspersky es uno de los antivirus gratuitos mejor valorados, permite analizar nuestros dispositivos en tiempo real o incluso llevar a cabo análisis de los mismos.

Visita la web[13] para conocer más información sobre sus planes.


Imagen 15: Kaspersky en Play Store

¿Qué puede llevar a cabo?

- Protección antivirus: actúa como una herramienta de limpieza de virus bloqueando el malware y mucho más automáticamente en tus teléfonos y tabletas.
- Comprobación en segundo plano: realiza un análisis a petición y en tiempo real en busca de virus, spyware, ransomware y troyanos.
- Localización del móvil: encuentra y bloquea nuestro teléfono Android o tablet en caso de pérdida o robo.
- Dónde está mi dispositivo: protege nuestra información personal de los ladrones, permitiendo borrarla de nuestro dispositivo remotamente.
- Bloqueo de aplicaciones: nos permite agregar un código secreto para acceder a mensajes privados o fotos, entre otros elementos.
- Antiphishing: protege nuestra información financiera cuando realizamos compras o transacciones bancarias online.

[13] https://www.kaspersky.es/

- Filtro web: filtra los enlaces y sitios peligrosos cuando navegamos por Internet.

- Dispositivos en mi red: nos avisa cuando un nuevo dispositivo se une a nuestra red Wi-Fi, para que podamos desconectar los dispositivos no autorizados.

Como podemos ver, la mayoría de los antivirus actuales nos ofrecen una protección completa e integral, el factor decisivo para decidirnos entre uno u otro depende del uso que hagamos de internet y de las funciones “extra” que podemos aprovechar de cada uno de ellos.

## 3.3. Alertas y consejos

Para terminar, tenemos unos últimos consejos para tener en cuenta.

### Consejos: Descarga segura de aplicaciones

A la hora de descargar aplicaciones es importante que lo hagamos desde las aplicaciones oficiales de descarga para nuestro dispositivo. Es necesario tener en cuenta que a pesar de que estas tiendas cuentan con filtros de protección estos no son 100% fiables, así a la hora de descargar las aplicaciones se recomienda:

1. Comprobar el número de descargas que tiene la aplicación, por lo general las aplicaciones con mayor número de descargas tienen una mayor probabilidad de ser reales.

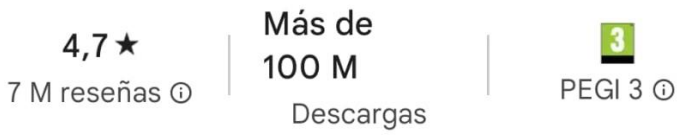


Imagen 16: Ejemplo número de descargas de una aplicación

2. Mirar los comentarios y reseñas, no es recomendable fiarse de aplicaciones con puntuaciones muy bajas o altas, a no ser que el número de reseñas sea elevado.


Imagen 17: Ejemplo de valoraciones y reseñas

3. Comprobar el creador de la aplicación. Una búsqueda rápida nos puede ayudar a tomar una decisión.

4. Comprobar qué permisos nos pide la aplicación una vez instalada, no debería pedir permisos a servicios que no necesita, por ejemplo, una aplicación para tomar fotos o vídeos no debería pedir permiso para acceder a los contactos del teléfono.

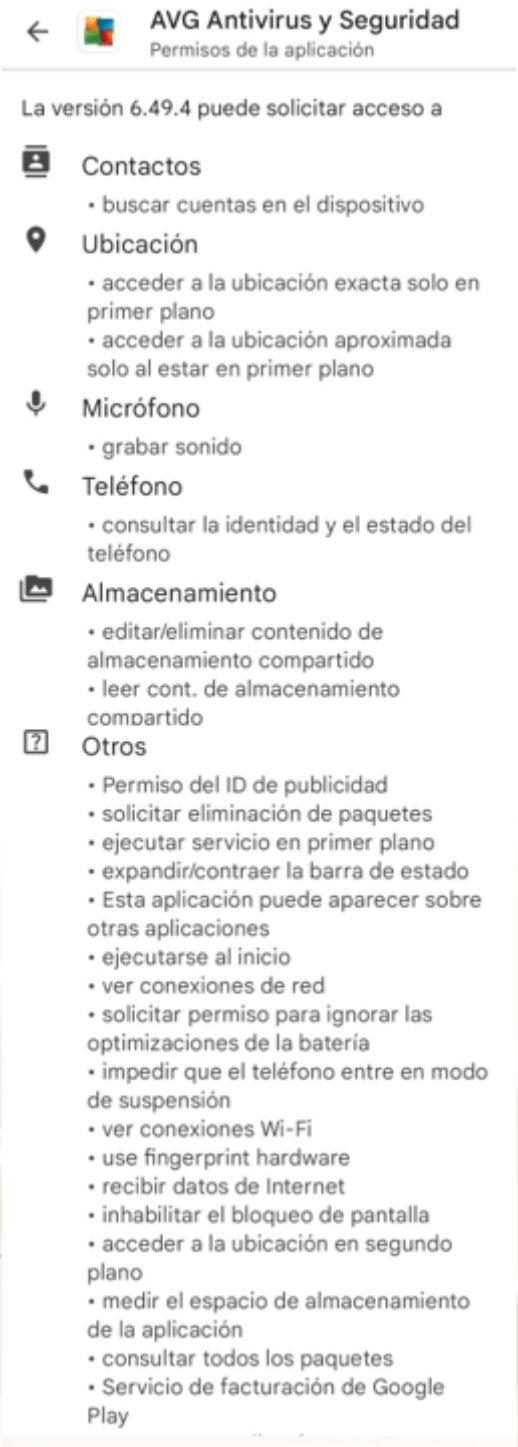


Imagen 18: Permisos que solicita la aplicación AVG

## Consejos: Mantén tu sistema operativo y antivirus actualizados

De la misma manera que van apareciendo nuevos métodos para intentar realizar nuevos tipos de ataques o engaños, las empresas que crean nuestros dispositivos también trabajan para mejorar su seguridad.

Para que estos nuevos métodos de protección de nuestros dispositivos tengan efecto es necesario cumplir una serie de consejos.

- Es recomendable que actualicemos proactivamente todos los sistemas operativos, programas y antivirus. Siempre que te lo pidan, acepta la actualización y reinicia el dispositivo.
- Cuenta con un programa antivirus instalado y siempre actualizado.
- Siempre será mejor tener un antivirus, aunque no sea de pago que no tener ninguna protección.
- No tener antivirus es equivalente a dejar las puertas y ventanas de tu casa siempre abiertas.
- Mantén constantemente actualizado el antivirus y nunca lo desactives.
- Siempre descárgate los antivirus del proveedor oficial.

De la misma manera es necesario tener actualizado nuestro sistema operativo, porque de una versión a la siguiente se solucionan fallos de seguridad que pudieran tener las anteriores. Vamos a ver cómo actualizar nuestros sistemas:

En Windows 10

1. Hacemos clic sobre el icono de Windows en la esquina inferior izquierda y pulsaremos sobre el icono de la rueda dentada o Configuración.

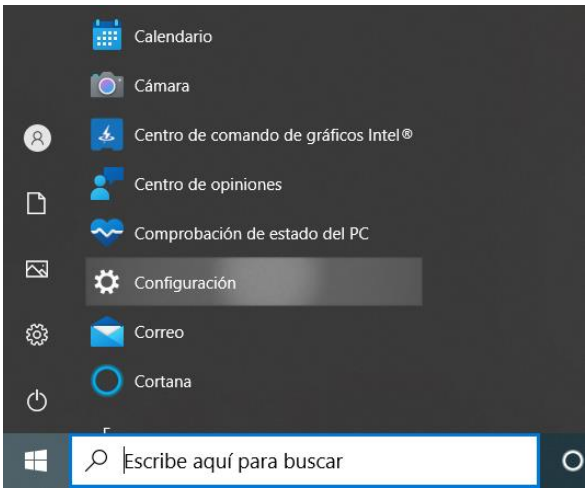


Imagen 19: Menú configuración Windows 10

2. En la nueva ventana, seleccionamos ‘Actualización y seguridad’ para acceder a sus opciones.


Imagen 20: Menú de configuración de Windows 10

3. Luego, dentro del apartado ‘Windows Update’, podremos ver si disponemos o no de la última versión. En caso de que nos aparezca el texto “No está todo actualizado” podremos hacer clic sobre ‘Buscar actualizaciones’ para descargar e instalar la última versión.

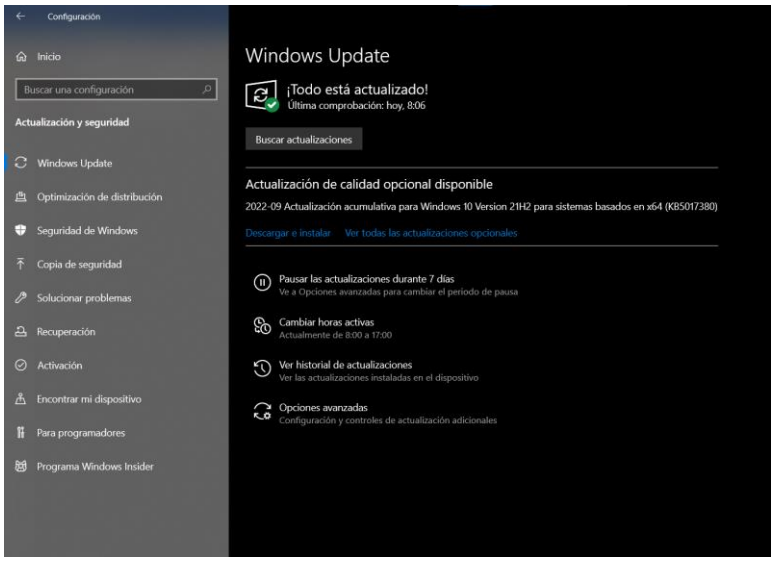


Imagen 21: Menú Windows update

4. Podemos seleccionar la opción de ‘Instalar actualizaciones tan pronto como sea posible’ para activar esta función e instalar cada actualización en el momento en que el fabricante la lance. Al finalizar la descarga e instalación, posiblemente nos solicite reiniciar el equipo. En ese caso, nos aseguraremos de cerrar cualquier programa que tengamos abierto y reiniciaremos.

En Android

En cada versión de Android y dispositivo puede variar ligeramente, pero los pasos esencialmente son los siguientes:

1. Lo primero que haremos será pulsar sobre el icono de ‘Ajustes’ de nuestro dispositivo.

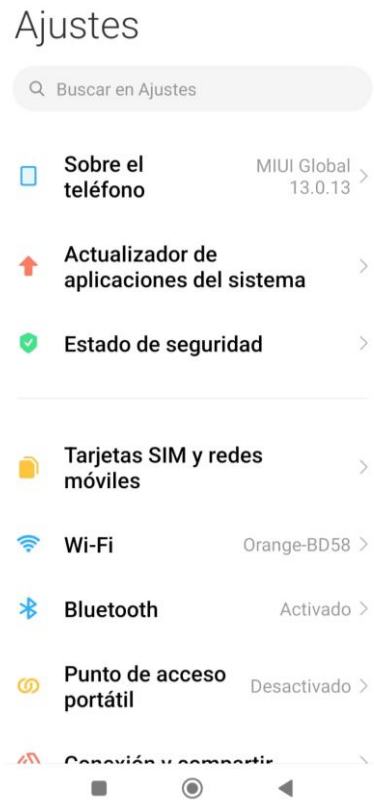


Imagen 22: Menú ajustes Android

2. Pulsamos en “sobre el teléfono”. Aquí podremos comprobar la versión de Android que tenemos instalada.


Imagen 23: Pantalla versión de Android en el teléfono

3. Si pulsamos en ‘Comprobar actualizaciones’, se iniciará la comprobación y, en caso de que haya una nueva versión disponible, podremos descargarla e instalarla.

En MacOS

Puede variar en cada versión de MacOS, pero los pasos a seguir suelen ser los siguientes:

1. Acceder al ‘menú de Apple > Preferencias del Sistema > Actualización de software’.


Imagen 24: Botón actualización de Software

2. Dentro, podremos comprobar las actualizaciones disponibles.

3. Si el mensaje que vemos nos indica que ‘Mac ya está actualizado’, eso implicará que tanto el sistema operativo, como todas las aplicaciones de Apple lo estarán.


Imagen 25: Versión del sistema operativo

4. Si, por el contrario, al hacer clic en ‘Actualizar ahora’, el mensaje nos indica que hay una actualización pendiente, podremos descargarla e instalarla en el momento.

5. Finalmente, para asegurarnos siempre de disponer la última versión actualizada, es recomendable marcar la casilla ‘Mantener mi Mac actualizado’. De este modo, recibiremos una notificación cada vez que haya una nueva versión pendiente de instalar.


Imagen 26: Activación de actualizaciones automáticas

En iOS

1. Iremos a ‘Ajustes > General y buscaremos la opción Actualización de software‘.


Imagen 27: Menú ajustes iOS

2. Aquí veremos nuestra versión actual de iOS. Si pulsamos sobre ‘Descargar e instalar’, comenzará la descarga de la nueva actualización. En caso contrario, nos informará que disponemos de la última versión.


Imagen 28: Actualizaciones automáticas iOS

3. Es recomendable activar la ‘Actualización automática’ del software del dispositivo. Cada vez que haya una nueva versión, nuestro dispositivo nos informará y podremos descargarla e instalarla en ese momento o más tarde.

4. Para actualizar todas aquellas aplicaciones que hemos instalado a través de la App Store, como redes sociales, juegos u otras aplicaciones. Para ello, deberemos volver al menú de ‘Ajustes > App Store’ y activar la función ‘Actualizaciones de apps’.

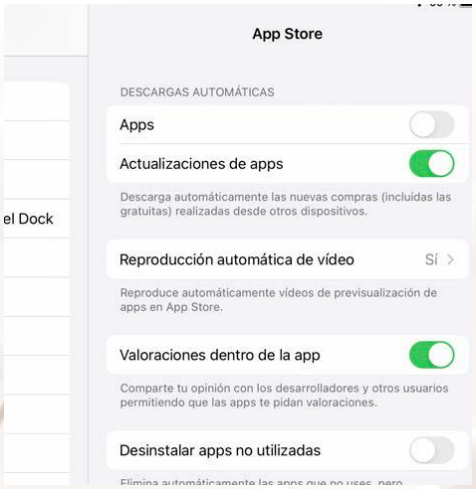


Imagen 29: Actualización automática de aplicaciones

## Consejos: Realiza copias de seguridad

Para evitar perder nuestros datos y archivos y proteger nuestra información es recomendable llevar a cabo copias de seguridad de nuestra información.

El caso ideal es realizar copias de seguridad de forma periódica ya sea de forma automática o manual que en caso de necesidad o pérdida de archivos por cualquier motivo te permita recuperarlos.

El caso ideal es tener tres copias de seguridad:

a. Una copia local en tu dispositivo.

b. Una copia cifrada en la nube. Para realizar copias de seguridad en la nube se pueden utilizar servicios como:

    - Google drive[14]
    - Dropbox[15]
    - OneDrive[16]

c. Una copia cifrada en un disco duro externo.

## Alerta: E-mails extraños

Una de las formas más sencilla de llegar hasta nosotros es a través de emails, por eso es necesario tener un poco de cuidado a la hora de abrir los emails que recibamos y tener en cuenta los siguientes consejos:

- Duda de todos los e-mails extraños o que no esperas recibir.
- Debes sospechar de todo email, ya te lo envíe una persona desconocida o una persona conocida, pero con un contenido atípico.

[14] https://drive.google.com/
[15] https://www.dropbox.com/
[16] https://onedrive.live.com/

Por lo general tenemos que estar especialmente atentos si:

1. No conocemos al remitente o lo conocemos, pero el contenido es atípico.
2. El nombre o dirección de correo del remitente contiene errores, es parcial o tiene una extensión diferente a la de su dominio principal.
3. Contiene errores de ortografía o gramaticales.
4. Nos ofrece una muy buena oferta, pide algo con cierta urgencia o que le facilitemos información.

En caso de sospechar de cualquier email seguiremos los siguientes pasos:

1. Revisaremos el remitente y el asunto, y si seguimos sospechando es mejor no abrirlo.
2. Si ya lo hemos abierto:
    a. No lo contestaremos.
    b. No descargaremos los archivos adjuntos.
    c. No haremos clic en ningún enlace ni imagen (pueden tener enlaces).
3. Lo clasificaremos como SPAM.
4. Si conocemos al remitente, contactaremos por otra vía (teléfono, whatsapp, etc.) para confirmar su veracidad.

## 3.4. Actividad 2

Actualiza el sistema operativo de tu Smartphone y comprueba que el antivirus está activado, en caso de no estarlo instala un antivirus.

# 04. Evaluación

Este último capítulo propone una última actividad dividida en dos partes, cada una de ellas se le estima una duración de 15 minutos.

## 4.1. Reflexión

En esta ronda de reflexión los participantes en el curso compartirán su opinión y plantearán las dudas que tengan, el educador recogerá las preguntas y se intentarán resolver en la siguiente parte.

## 4.2. Ronda de dudas

Las dudas, comentarios o sugerencias sobre el curso, la aplicación o la página web se habrán recogido por el educador y entre todos intentarán resolverlas. En caso de no poder resolver alguna de las dudas se les enviará una respuesta por email a los participantes.

# 05. Anexo

## 5.1. Enlaces y referencias

Páginas Webs importantes:

- Sellos de confianza online[17]
- Test de ciberseguridad[18]
- Test de compras por internet[19]
- Instituto nacional de ciberseguridad[20]
- Política de Google de Software No Deseado[21]
- Manual de experiencia senior en ciberseguridad[22]
- Google drive[23]
- Dropbox[24]
- OneDrive[25]

[17] https://protecciondatos-lopd.com/empresas/sellos-de-confianza-online/
[18] https://www.incibe.es/ciudadania/formacion/autoevaluacion
[19] https://www.incibe.es/ciudadania/formacion/autoevaluacion
[20] https://www.incibe.es/
[21] https://www.google.com/about/unwanted-software-policy.html
[22] https://www.incibe.es/sites/default/files/docs/senior/guia_ciberseguridad_para_todos.pdf
[23] https://drive.google.com/
[24] https://www.dropbox.com/
[25] https://onedrive.live.com/