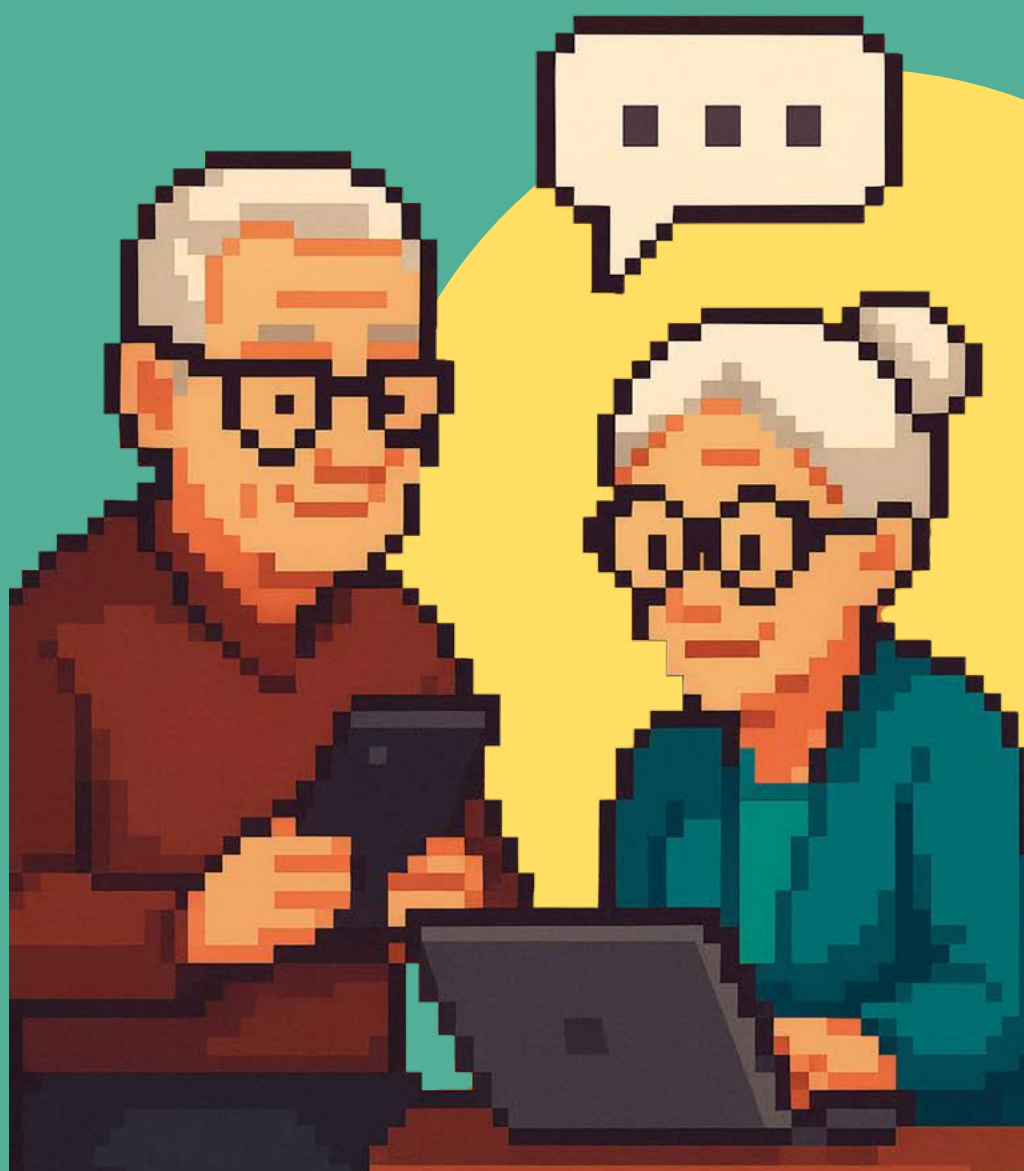




Guía de Seguridad Digital

Para Personas Mayores



Junta de Andalucía
Consejería de Inclusión Social,
Juventud, Familias e Igualdad

www.juntadeandalucia.es

ÍNDICE

1. Introducción	5
1.1 Sobre esta guía	5
1.2 ¿Por qué a las personas mayores nos importa la seguridad digital?	6
1.3 La seguridad digital de las personas mayores en Andalucía	7
2. Primeros pasos con la tecnología	9
2.1 Breve introducción a las TIC	10
2.2 Configuración inicial del dispositivo	12
2.3 Ajustes de seguridad	21
2.4 Descarga e instala aplicaciones de forma segura	25
3. Seguridad digital básica en el uso diario	29
3.1 ¿Cómo crear y mantener contraseñas seguras?	29
3.2 Protección frente a riesgos comunes en Internet	31
4. Seguridad en Internet y redes sociales	40
4.1 Navegación segura en Internet	40
4.2 Uso seguro de las redes sociales: Facebook e Instagram	42
4.3 Uso seguro de las aplicaciones de comunicación instantánea: conversaciones, videollamadas y reuniones en línea	46
5. Trámites y compras por Internet	56
5.1 Certificado digital	56
5.2 Cómo pido una cita previa de forma segura	58
5.3 Compras Online	61

6. Uso responsable del correo electrónico	65
6.1 ¿Qué es un correo electrónico y cómo funciona?	65
6.2 Detecta correos sospechosos o fraudulentos	69
7. Qué hacer si tengo un problema	72
7.1 Concepto de identidad digital y cómo protegerla	72
7.2 ¿Qué hacer si me han estafado?	74
7.3 ¿Qué hacer si han suplantado mi identidad?	76
8. Inteligencia Artificial para un envejecimiento activo seguro	79
8.1 Configura de forma segura el Asistente Virtual tu móvil: Google	80
8.2 Configura de forma segura un Asistente Virtual en casa: Alexa	82
8.3 Configura las notificaciones de aplicaciones y juegos para evitar publicidad engañosa, estafas y cobros no deseados	84
9. Mantenimiento y respaldo de información	86
9.1 Copia de seguridad	86
9.2 Limpieza de archivos obsoletos y del caché	89
10. Recursos y redes de apoyo	92
10.1 Teléfonos y páginas de ayuda oficial	92
10.2 Canales y servicios para la inclusión digital de personas mayores	93
11. Glosario de términos sobre Seguridad Digital	94

1. INTRODUCCIÓN

La tecnología forma parte de nuestra vida diaria. Usamos el móvil para conectarnos con familiares y amistades, Internet para realizar gestiones o trámites, y las redes sociales para socializar o como medio de entretenimiento, entre otras. Todo esto nos ofrece muchas ventajas, pero también podemos sufrir riesgos si no sabemos como protegernos digitalmente.

1.1 Sobre esta guía

Esta Guía de Seguridad Digital para Personas Mayores, realizada por la Junta de Andalucía, Consejería de Inclusión Social, Juventud, Familias e Igualdad, a través de la Dirección General de Personas Mayores, Participación Activa y Soledad no deseada, ha sido diseñada para acompañarte, paso a paso, en un uso seguro de la tecnología, con un lenguaje sencillo, explicaciones claras y ejemplos prácticos. Así que no necesitas conocimientos previos para comenzar a leerla.

↑
ÍNDICE

Aquí, te explicamos todos los conceptos más utilizados en el mundo de la seguridad digital. Cada uno va acompañado de un ejemplo práctico, para que puedas practicar con tu dispositivo y comprendas mejor su utilidad. Al final de la guía encontrarás un glosario para que consultes los términos tecnológicos utilizados más relevantes.

Además, esta guía, está hecha para que la leas como prefieras. Puedes avanzar a tu ritmo, comenzar desde el principio o ir directamente al tema que más te interese, para que le saques el máximo partido.

También, la tecnología se aprende en compañía. Te invitamos a que compartas esta guía con tus familiares, amistades y toda aquella persona que creas que le pueda interesar. Tú decides cómo hacerlo y cuándo avanzar. No importa tu edad, aprender algo nuevo es posible, útil y te da confianza.

1.2

¿Por qué a las personas mayores nos importa la seguridad digital?

A las personas mayores nos importa la seguridad digital porque cada vez utilizamos más la tecnología en nuestra vida diaria. Conocer cómo proteger nuestros datos y usar Internet de forma segura a través de nuestros dispositivos nos ayuda a evitar engaños, cuidar nuestra privacidad y sentirnos con más tranquilidad y confianza. Por eso, es importante conocer las principales razones por las que la seguridad digital es fundamental para nuestro bienestar:

1. Mayor vulnerabilidad ante fraudes y engaños

Las personas mayores somos uno de los grupos más vulnerables ante las estafas en línea. Esto se debe a que:

- Podemos no estar familiarizadas con tecnologías o tácticas engañosas como el phishing, la suplantación de identidad o los fraudes por mensajes.
- Confiamos con más facilidad, y eso, puede aumentar el riesgo de fraudes y engaños.



ÍNDICE

2. Mayor uso de servicios digitales sin formación previa

Muchas personas mayores hemos comenzado a usar las tecnologías en etapas más avanzadas de nuestras vidas, sin haber tenido una educación digital formal antes:

- Accedemos a trámites gubernamentales, bancarios o de salud en línea.
- Utilizamos redes sociales o de mensajería sin saber cómo proteger nuestra información.

3. Riesgo económico

Un ataque digital puede implicar:

- Pérdida de nuestros ahorros o pensiones.
- Contrataciones de servicios sin nuestro consentimiento.
- Fraude con tarjetas, Bizum o la suplantación de nuestra identidad en plataformas de pago.

4. Pérdida de confianza en la tecnología

Un mal uso o una mala experiencia puede llevarnos a:

- Rechazar o temer el uso de herramientas digitales.
- Aislamiento social si dejamos de comunicarnos por medios digitales con nuestros familiares o servicios.

5. Autonomía e inclusión social

La seguridad digital es una herramienta para la autonomía:

- Nos permite hacer trámites, comunicarnos y acceder a servicios sin depender de terceras personas.
- Fortalece nuestro derecho a participar plenamente en la sociedad digital.

1.3

La seguridad digital de las personas mayores en Andalucía

↑
ÍNDICE

En 2024, Andalucía experimentó un notable incremento en los fraudes a través de Internet, consolidándose como la comunidad autónoma con mayor incidencia de fraudes Online en España.

Según los datos publicados en el Balance de Criminalidad del Ministerio del Interior, Andalucía registró la mayor cifra de infracciones penales relacionadas con estafas informáticas y ciberdelitos, llegando a 81.559 casos, lo que representa, aproximadamente, un 20% del total de infracciones penales en la región.

En cuanto a los datos por provincias, Sevilla (19.372), Málaga (18.258) y Cádiz (12.504) son las que más infracciones registraron. Por el contrario, las provincias que menos casos de ciberestafas acumularon son Huelva (3.537), Jaén (4.971) y Almería (5.915). Además, en las provincias de Córdoba (7.460) y Granada (9.542) se ha observado un ligero descenso de este tipo de delitos en su comparativa con los datos del año 2023.

La seguridad digital comienza con pequeños gestos cotidianos.



Del total de los ciberdelitos registrados en 2024, 71.327 casos correspondieron a estafas informáticas, consolidándose éstas como el tipo de delito cibernético más común. También, se registraron más de 40.000 denuncias por phishing bancario, una técnica que consiste en la suplantación de identidad para obtener datos personales y bancarios, haciendo que la cibercriminalidad haya incrementado durante el 2024 en un 0,28% en Andalucía.

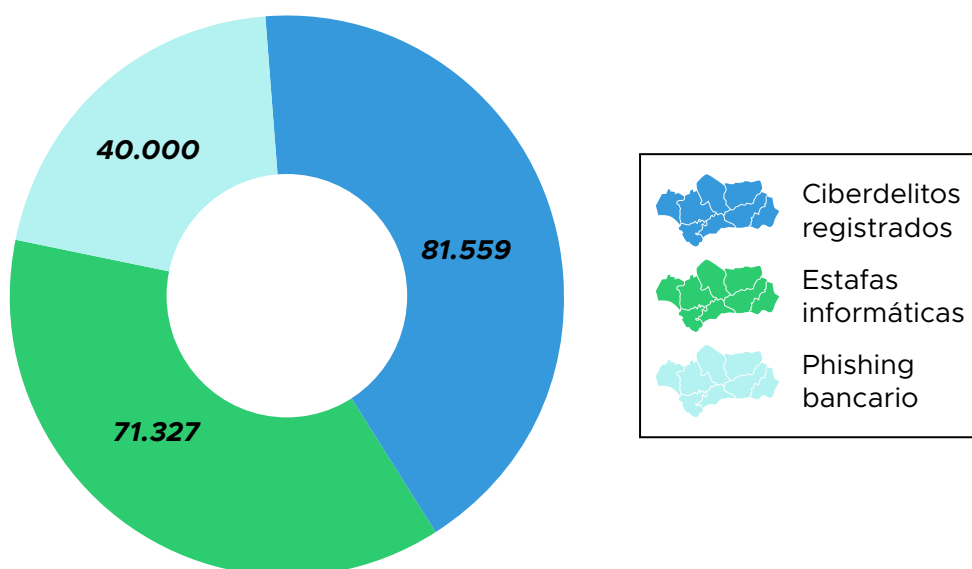


ÍNDICE

Datos sobre criminalidad en internet

Fraudes online en Andalucía (2024)

Fuente: Ministerio del Interior



En resumen, cuidar nuestra seguridad digital va más allá de aspectos técnicos. Una buena formación en seguridad digital nos permite desenvolvernos con mayor confianza y autonomía, y nos protege frente a los riesgos presentes en el entorno digital.

2. Primeros pasos con la tecnología

Cuando nos adentramos en el mundo de las tecnologías y la seguridad digital, nos encontramos con muchas palabras nuevas que no entendemos. Ésto nos dificulta comprender el funcionamiento lógico de los dispositivos móviles, al igual que las posibilidades que éstos nos ofrecen. Por ello, es importante, que conozcamos los conceptos e ideas principales que se usan dentro de la seguridad digital, así como aprender a configurar los dispositivos para adaptarlos a nuestras capacidades y necesidades.

Usar el móvil con seguridad te da más libertad y tranquilidad.



↑
ÍNDICE

2.1

Breve introducción a las TIC

1. ¿Qué son las TIC?

Las TIC son las Tecnologías de la Información y la Comunicación. Son todas aquellas herramientas que usamos para comunicarnos, buscar información, aprender y hacer gestiones a través de medios digitales.

Incluyen, por ejemplo:



**Teléfonos
móviles y
smartphones**



**Ordenadores
y tablets**



Internet



**WhatsApp,
Facebook o
videollamadas**



**Plataformas para
comprar o hacer
gestiones online**



**Trámites online
como pedir cita
médica o hacer la
declaración de la
renta**



ÍNDICE

2. ¿Por qué son importantes en nuestra vida diaria?

Las Tecnologías de la Información y la Comunicación (TIC) forman parte de nuestra vida diaria. Las podemos usar para estar en contacto con familiares y amistades, nos permiten hacer gestiones sin salir de casa, como pedir una cita previa o pagar un recibo, nos facilitan aprender cosas nuevas, leer las noticias o ver vídeo-tutoriales. También, las podemos usar para solicitar ayudas o firmar documentos digitalmente. Y aunque al principio nos pueda resultar complicado y difícil, nunca es tarde para que las personas mayores aprendamos a usarlas de forma segura, para vivir con más autonomía, seguridad y conexión con el mundo.



**La tecnología
también es tuya:
tómatala con
calma y
curiosidad**

↑
ÍNDICE

2.2 Configuración inicial del dispositivo

Antes de comenzar a usar tu móvil, es importante realizar una configuración básica para que nos resulte seguro, cómodo y fácil de usar. Aquí te explicamos paso a paso cómo hacerlo.

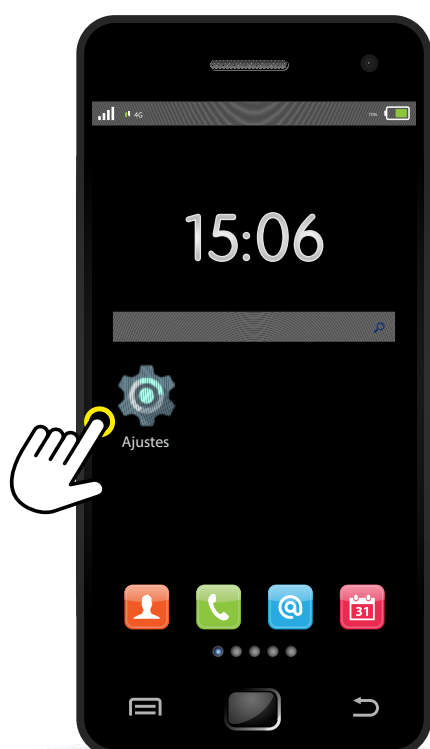
Si te cuesta leer la pantalla de tu teléfono porque las letras son pequeñas, puedes aumentar el tamaño de la letra para ver mejor los mensajes, menús y aplicaciones.

1. Pasos para aumentar el tamaño de la letra en Android:

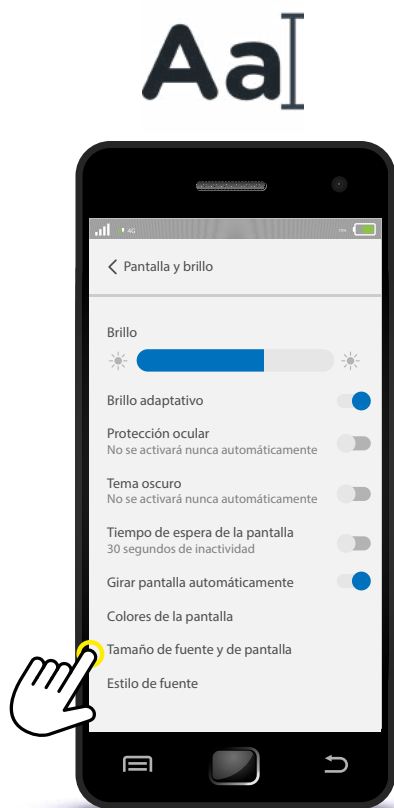
1. Abre la aplicación de “Ajustes” (El icono es una rueda dentada).

2. Desliza hacia abajo y pulsa en “Pantalla” (En algunos móviles puede llamarse “Visualización”).

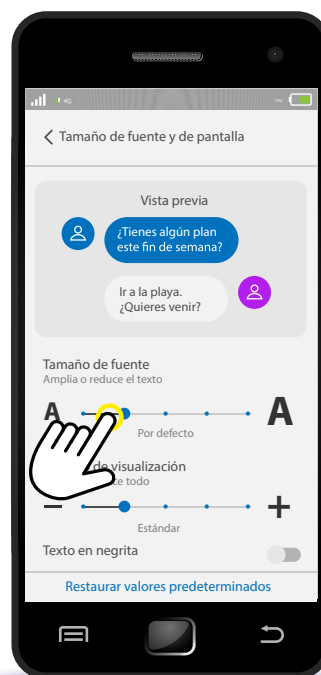
↑
ÍNDICE



3. Busca y pulsa la opción “Tamaño de fuente” o “Tamaño del texto”.



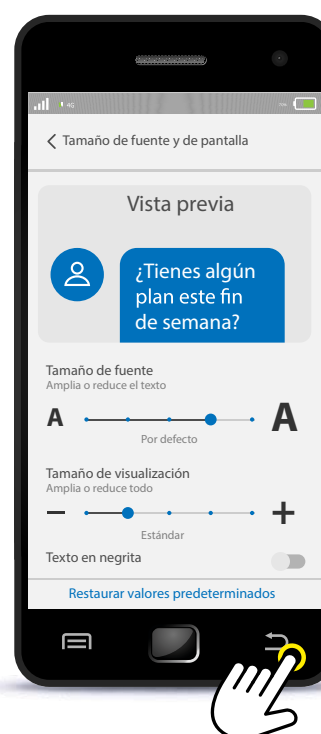
4. Ajusta el tamaño de la letra moviendo el control deslizante hacia la derecha (más grande) o hacia la izquierda (más pequeño).



5. Verás una vista previa del texto. Elige el tamaño que te resulte más cómodo.



6. Cuando lo tengas, vuelve atrás o cierra ajustes. El cambio se guarda automáticamente.



↑
ÍNDICE

Consejos útiles:



Después probar diferentes tamaños hasta encontrar el que resulte más fácil de leer

N

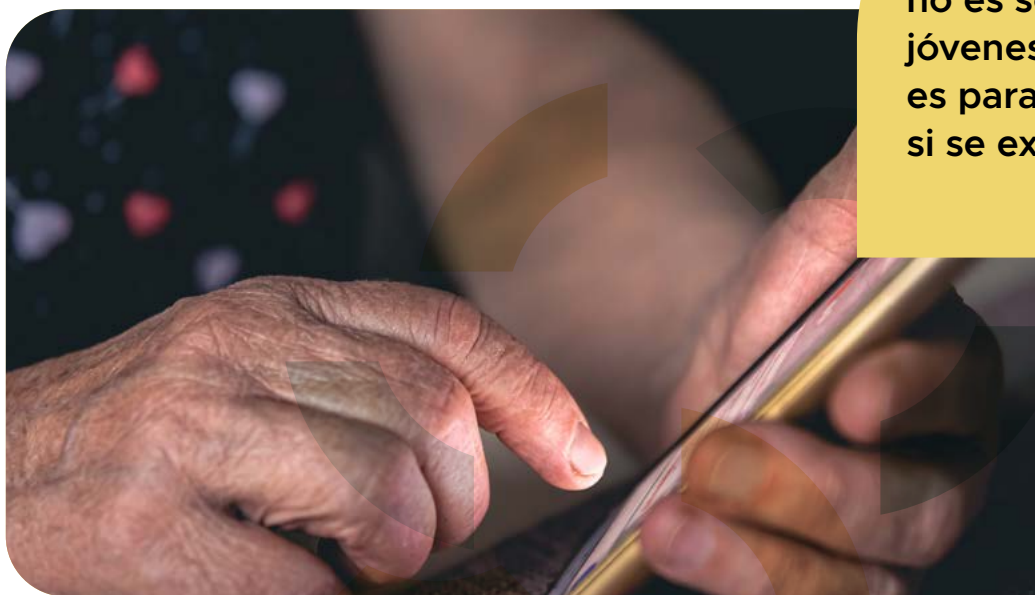
También puedes activar el modo de alto contraste o texto en negrita en la selección de Accesibilidad si necesitas mayor visibilidad

Resultado:

Después de hacer este cambio, todo lo que leas en tu móvil será más grande y claro, incluyendo mensajes, menús y aplicaciones



ÍNDICE



La tecnología no es solo para jóvenes. También es para mayores, si se explica bien

2. ¿Cómo ajustar el brillo de la pantalla para leer mejor el móvil?

El brillo de la pantalla es la luz que emite tu teléfono. Si está muy bajo, puede costarte leer; si está muy alto, puede molestar a los ojos, sobre todo de noche. Ajustarlo te ayudará a leer mejor y cuidar tu vista.



Opción 1: Desde la pantalla principal (método rápido)

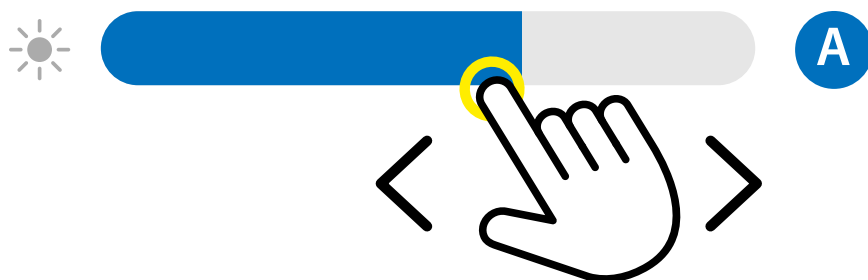
1. Desliza un dedo desde la parte superior de la pantalla hacia abajo para abrir el menú rápido.

↑
ÍNDICE

2. Busca el icono del sol  o una barra con un control deslizante.

3. Desliza el control hacia la derecha para aumentar el brillo (más claro) o hacia la izquierda para reducirlo (más oscuro).

4. Puedes ajustar el brillo las veces que necesites, según la luz del lugar.



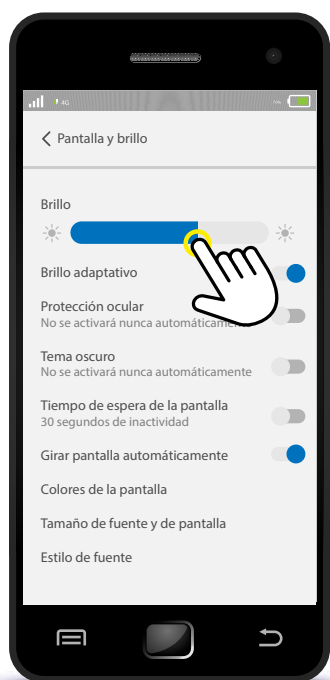
Opción 2: Desde los ajustes del teléfono

1. Abre la App de “Ajustes” (icono de rueda dentada ).
2. Pulsa en “Pantalla” o “Visualización”.
3. Entra en la opción “Brillo” o “Nivel de brillo”.
4. Ajusta el control de brillo según tu comodidad.

Opción 3: “Brillo Automático”

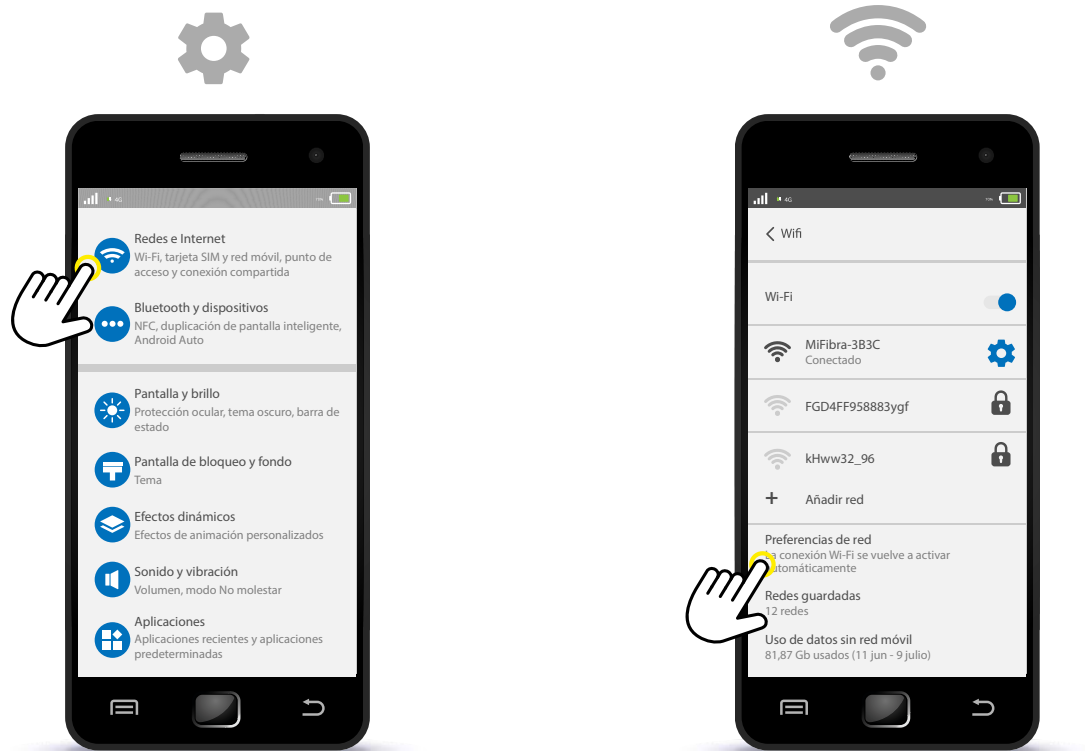
Esta opción ajusta el brillo de la pantalla de manera automática, en función de la luz que haya en cada momento. Actívalo repitiendo los pasos de la Opción 2 o desde Ajustes > Pantalla > Brillo automático. Si prefieres ser tú quien controle el brillo, déjalo desactivado.

↑
ÍNDICE



3. ¿Cómo conectarte a una red Wi-Fi de forma segura?

Conectar tu móvil, tableta u ordenador a una red Wi-Fi te permite navegar por Internet sin gastar datos móviles. Pero hacerlo de forma segura es muy importante para proteger tu información.



1. Abre “Ajustes” (icono de engranaje ).
2. Pulsa en “Redes” o “Wi-Fi”.
3. Asegúrate de que el interruptor esté en “Activado”.

4. Verás una lista de redes. Pulsa sobre el nombre de la red Wi-Fi que prefieras. El nombre de la red Wi-Fi suele estar escrito en una pegatina en el router.

5. Introduce la contraseña, suele estar escrita en una pegatina en el router, junto a la palabra “clave” o “password”.



En este router la pegatina está arriba, pero en otros puede estar debajo y tendrás que darle la vuelta.

6. Pulsa en “Conectar”.



Marca la opción de “conectar automáticamente” si la red es de tu confianza y así no tendrás que repetir este proceso cada vez que quieras conectarte



ÍNDICE



Consejo para una conexión segura

- Usa siempre que puedas tu red personal de casa, nunca redes públicas abiertas (como Wi-Fi de bares o plazas) para trámites importantes.

4. Importancia de tener instalado un antivirus

El antivirus es como un guardia que protege tu dispositivo de virus, estafas, aplicaciones peligrosas y accesos no deseados.

¿Por qué es necesario?



Te avisa si una aplicación es sospechosa



Evita que te entren virus o programas espía



Protege tus datos personales y bancarios

¿Cuándo lo instalo?



Desde el primer día que uses tu dispositivo



Justo después de conectarte a Internet

↑
ÍNDICE

Consejos al elegir un antivirus gratuito



- **Actualizaciones automáticas:** Asegúrate de que el antivirus mantenga sus definiciones de virus siempre actualizadas
- **Protección en tiempo real:** Es decir, que vigile constantemente tu dispositivo, no solo cuando haces un escaneo manual
- **Instalar solo desde fuentes oficiales:** Descarga el antivirus desde la web del proveedor o desde tiendas oficiales (Google Play / App Store)

¿Qué antivirus puedo usar?

Hay muchos antivirus para descargar. Los siguientes nos ofrecen una protección básica contra virus y amenazas comunes sin necesidad de pagar. Recuerda que debes mantener el antivirus actualizado y escanear tu dispositivo, al menos, una vez por semana.

Antivirus más conocidos



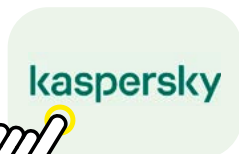
- **Bitdefender Antivirus Free:** Buena protección contra virus y malware, funciona en segundo plano, ideal si te estás iniciando en el mundo digital.



- **Avast Free Antivirus:** Nos ofrece una protección en tiempo real y funciones adicionales como el escaneo de red y el bloqueo de enlaces peligrosos.



- **AVG AntiVirus Free:** Comparte el mismo motor de protección que Avast y es fácil de usar, con escaneos automáticos y protección contra descargas maliciosas.



- **Kaspersky Security Cloud Free:** Buen equilibrio entre simplicidad y funciones, con protección en tiempo real y escaneo de enlaces.



- **Windows Defender (Microsoft Defender Antivirus):** Antivirus gratuito integrado en Windows 10/11, se ejecuta automáticamente y protege el sistema sin necesidad de instalar nada extra.

Antivirus para móviles

Muchos de los anteriores (como Avast, AVG, Avira y Kaspersky) también tienen versiones gratuitas para **Android** o **iOS**. Estas versiones nos ayudan a bloquear aplicaciones maliciosas, escanear archivos sospechosos y proteger la navegación web. En Android, además de un antivirus, **Google Play Protect** viene integrado y realiza escaneos automáticos de las aplicaciones instaladas desde la tienda oficial.

2.3

Ajustes de seguridad

1. ¿Por qué es importante?

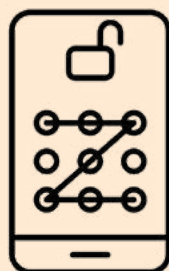
Para que solo tú puedas acceder a tu teléfono y proteger tu información personal.

Pasos recomendados:

1. Ve a Ajustes > Seguridad o Pantalla de bloqueo.
2. Elige un método de seguridad:



PIN
(4 dígitos que solo tú sepas)



Patrón
(dibujar una forma)



Huella dactilar o facial
(si tu teléfono lo permite)

↑
ÍNDICE

3. Activa la opción de bloqueo automático después de unos minutos sin uso.



Usa un PIN fácil de recordar pero difícil de adivinar
(no uses tu año de nacimiento)

2. Activación del bloqueo de pantalla

Activar el bloqueo de la pantalla es muy importante para proteger la información de tu dispositivo, sobre todo si pierdes el teléfono o si alguien quiere usarlo sin tu permiso.

Pasos recomendados:

1. Ve a Ajustes > Pantalla > Suspensión o bloqueo automático.
2. Activa que el teléfono se bloquee después de 30 segundos o 1 minuto sin uso.
3. Verifica que al encender la pantalla, te pida el PIN o huella.
4. Puedes apagar manualmente la pantalla pulsando el botón lateral del teléfono.

3. ¿Qué es un cortafuegos o firewall?



ÍNDICE

El cortafuegos, también llamado firewall en inglés, es como un portero digital que vigila lo que entra y sale de tu dispositivo a través de Internet.



¿Para qué sirve?

- Controla y bloquea conexiones peligrosas que intentan acceder a tu móvil u ordenador.
 - Evita que programas maliciosos (virus, espías, estafas) salgan o entren sin tu permiso.
 - Es una primera línea de defensa junto al antivirus.
- Imagina que tu dispositivo es tu casa. El cortafuegos sería la puerta cerrada con llave que solo se abre a personas de confianza.



¿Lo tengo activado?

↑
ÍNDICE

- En Windows, el cortafuegos viene activado por defecto.
- En móviles Android, estas funciones ya están integradas, pero puedes reforzarlas con otras aplicaciones de seguridad.



No desactives el cortafuegos si no sabes lo que estás haciendo. Déjalo activo siempre

4. ¿Por qué es importante que tu dispositivo esté actualizado?

Las actualizaciones del sistema y de las aplicaciones corrigen errores, agregan mejoras... ¡y también tapan agujeros de seguridad!

¿Qué pasa si no está actualizado?

- Tu dispositivo queda más vulnerable a ataques o estafas digitales.
- Algunas aplicaciones pueden dejar de funcionar bien.
- Puedes perder funciones importantes de seguridad o privacidad.

¿Cómo activar las actualizaciones automáticas?



Android

1. Ve a Play Store



2. Pulsa en tu foto o inicial, luego en “Ajustes”

3. Entra en “Preferencias de red” > “Actualizar Apps automáticamente”

4. Selecciona: “Solo por Wi-Fi” (para no gastar datos móviles)



Deja el equipo conectado y encendido una vez a la semana para que pueda actualizarse solo



Windows

1. Abre Inicio > Configuración

2. Ve a “Actualización y seguridad”

3. Asegúrate de que las actualizaciones estén activadas y configuradas para instalarse automáticamente



Tener el cortafuegos activado y las actualizaciones automáticas encendidas es como tener una casa con cerradura moderna y mantenimiento regular. Son pasos sencillos que te protegen todos los días sin que tengas que hacer nada complicado

2.4

Descarga e instala aplicaciones de forma segura

1. ¿Por qué es importante?

La importancia de tener aplicaciones oficiales en nuestro dispositivo es fundamental para evitar virus, estafas o aplicaciones falsas que roban datos. Evita instalar Apps desde mensajes, enlaces desconocidos o páginas que no sean oficiales.

Para evitar instalar programas peligrosos, es muy importante que descargues tus aplicaciones sólo desde las tiendas oficiales, como:



Google Play Store
(si usas un móvil Android)



App Store
(si usas un iPhone o iPad)

↑
ÍNDICE

Estas tiendas revisan las aplicaciones antes de publicarlas, por eso son más seguras que páginas web o enlaces que te mandan por mensaje.

2. ¿Cómo descargar aplicaciones?

Pasos recomendados:

1. Abre la Play Store (icono con un triángulo de colores en Android) o App Store (icono con una “A” azul si usas un iPhone o iPad).
2. Usa la barra de búsqueda para encontrar Apps conocidas (por ejemplo: WhatsApp, Gmail, Google Maps).



WhatsApp



Gmail



Google Maps

3. Antes de descargar e instalar la aplicación fíjate que:

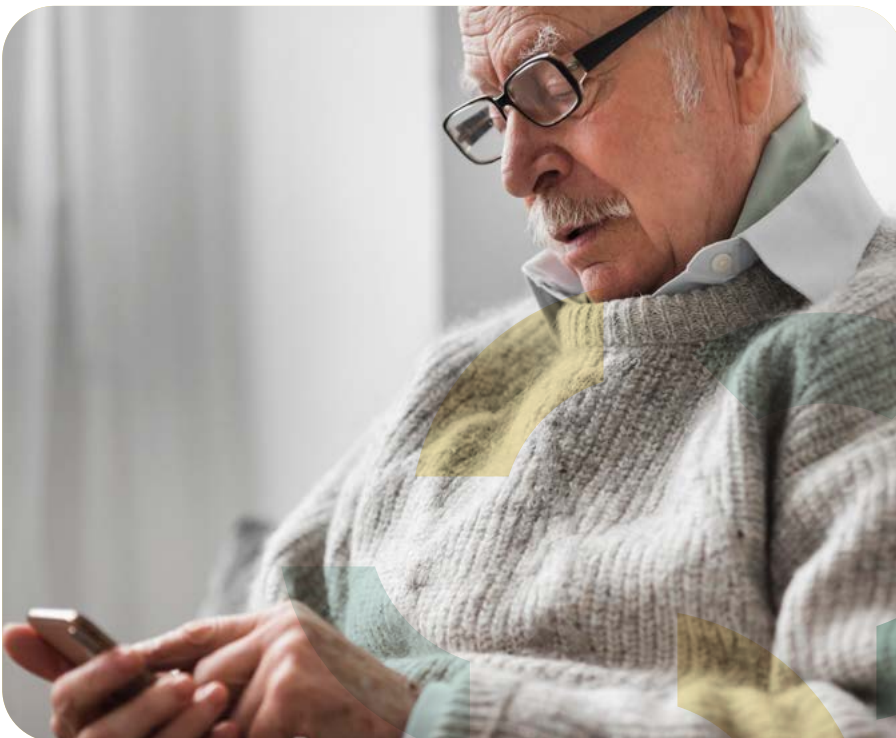
- El nombre del desarrollador sea oficial (por ejemplo: WhatsApp LLC).
- Tenga muchas descargas y buenas valoraciones (estrellas).

4. Pulsa en “Instalar”.



Nunca descargues aplicaciones desde enlaces sospechosos, correos o mensajes desconocidos

↑
ÍNDICE



3. ¿Qué son los permisos que piden las aplicaciones?

Cuando instalas una aplicación, esta puede pedirte permisos especiales para acceder a funciones de tu teléfono. Esto es normal, pero debes leer con atención qué permisos solicita y si tienen sentido.

Ejemplos comunes de permisos:

Permisos que piden	¿Para qué sirven?	Aplicaciones
Cámara 	Para sacar fotos o hacer videollamadas	 WhatsApp  Zoom  Meet
Micrófono 	Para enviar audios o hablar en llamadas	 WhatsApp  Telegram  Grabadora
Ubicación 	Para darte indicaciones o mostrar tu ubicación	 Google Maps
Contactos 	Para saber quién de tus contactos usa la app	 WhatsApp  Telegram
Archivos 	Para guardar o enviar fotos y documentos	 Gmail  Drive

↑
ÍNDICE



Si una App pide algo que no tiene sentido (por ejemplo, una linterna que pide tus contactos), no la instales



Da permisos solo cuando sea necesario



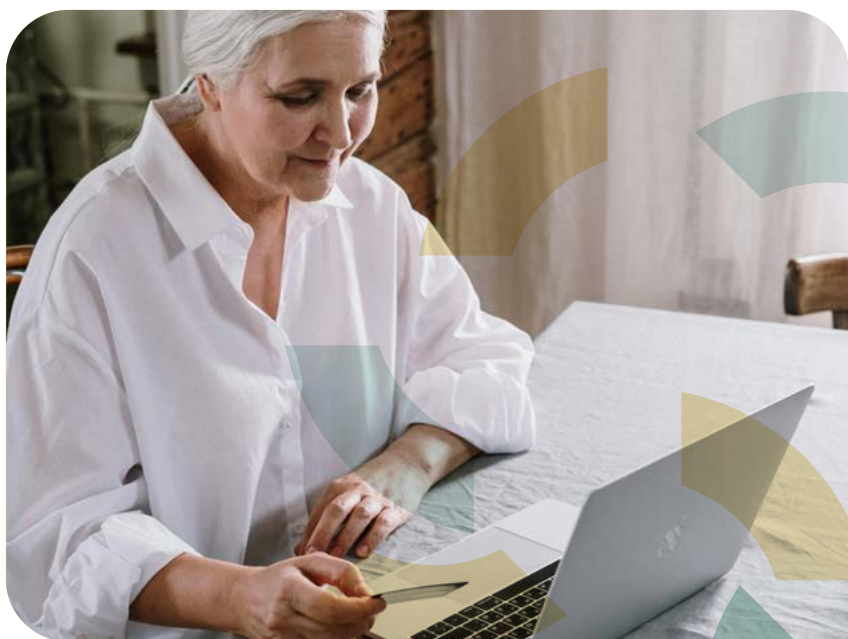
Puedes revisar o cambiar los permisos más tarde desde: Ajustes > Aplicaciones > [Nombre de la App] > Permisos



Descargar solo desde tiendas oficiales y entender qué permisos das es una forma sencilla de proteger tu privacidad y tu dispositivo



ÍNDICE



3. Seguridad digital básica en el uso diario

En el uso diario del móvil o el ordenador, hay pequeños gestos que te protegen de fraudes, pérdidas de información o accesos no deseados. Aquí te explicamos los más importantes.

3.1

¿Cómo crear y mantener contraseñas seguras?

1. ¿Por qué es importante?

Las contraseñas protegen tu correo, tus cuentas bancarias, redes sociales y toda tu información digital.

Consejos para crear una contraseña segura:

- Que tenga al menos 8 caracteres.
- Combina letras, números y símbolos.
- Evita usar datos personales (como tu nombre, fecha de nacimiento o DNI).

↑
ÍNDICE



2. Gestión de contraseñas

¿Qué hacer si no puedes recordar tantas contraseñas?

Opciones seguras:

- Anota tus contraseñas en un papel y guárdalo en un lugar privado (una caja o cajón personal).
- Usa un gestor de contraseñas (programa que guarda tus contraseñas de forma segura). Funciona con una sola contraseña maestra para entrar. Ejemplos: Google Passwords y Bitwarden.
- No compartas tus contraseñas con nadie, a menos que sea alguien de total confianza.



Es la herramienta gratuita que ofrece Google para guardar, recordar y proteger nuestras contraseñas de forma automática cuando usamos el móvil, la tablet o el ordenador.

↑
ÍNDICE



Gestor de contraseñas muy completo, ya que permite guardar contraseñas ilimitadas, generar nuevas contraseñas seguras y sincronizarlas entre distintos dispositivos (móvil, ordenador y navegador).

3. Uso seguro en dispositivos públicos o compartidos

Un dispositivo compartido es un móvil, tablet u ordenador que no es exclusivamente tuyo, sino que éste puede ser usado por otras personas. Por ejemplo, el dispositivo de una biblioteca, un centro cívico o de uso familiar.

Precauciones importantes:

- No guardes contraseñas ni marques “recordar contraseña”.
- No dejes tu sesión abierta. Cierra siempre tu sesión después de usar una cuenta (correo, redes, banco).
- Borra tu historial de navegación después de usar el navegador web.



Recuerda, en dispositivos públicos, evita hacer gestiones bancarias o personales

3.2

Protección frente a riesgos comunes en Internet

En Internet, al igual que en la vida real, también existen personas malintencionadas que intentan engañar, robar información o dinero. Conocer cómo funcionan estas trampas digitales te ayudará a protegerte y navegar con seguridad.

1. Diez consejos generales para tu seguridad digital

1. Protege tus cuentas en Internet: Crea contraseñas seguras y cámbialas con frecuencia. No uses la misma para todo. Anota todas tus contraseñas en un lugar privado

2. Realiza tus compras Online en páginas y aplicaciones de confianza y consultando las experiencias de clientes anteriores en los comentarios antes de realizar la compra

3. Evita abrir los correos electrónicos que no vayan dirigidos a ti o con asuntos extraños que te generen dudas. Estos correos te llevan a otras páginas malintencionadas para introducir nuestros datos personales

4. Protege el acceso a la información de tu dispositivo con un desbloqueo de pantalla y haz copias de seguridad periódicamente

5. Si te conectas a Internet desde una red Wi-Fi abierta, compartida o pública hay que evitar usar servicios que conlleven identificación o información personal

6. Protege la red de tu casa con los protocolos de seguridad de tu proveedor de Internet

↑
ÍNDICE

7. Vigila también la seguridad de los aparatos que hayas incorporado últimamente a Internet. Muchos de los aparatos electrónicos que existen hoy tienen la posibilidad de conectarse a la Red

8. Actualiza el software básico y complementos de tu dispositivo para disponer de las últimas versiones de seguridad

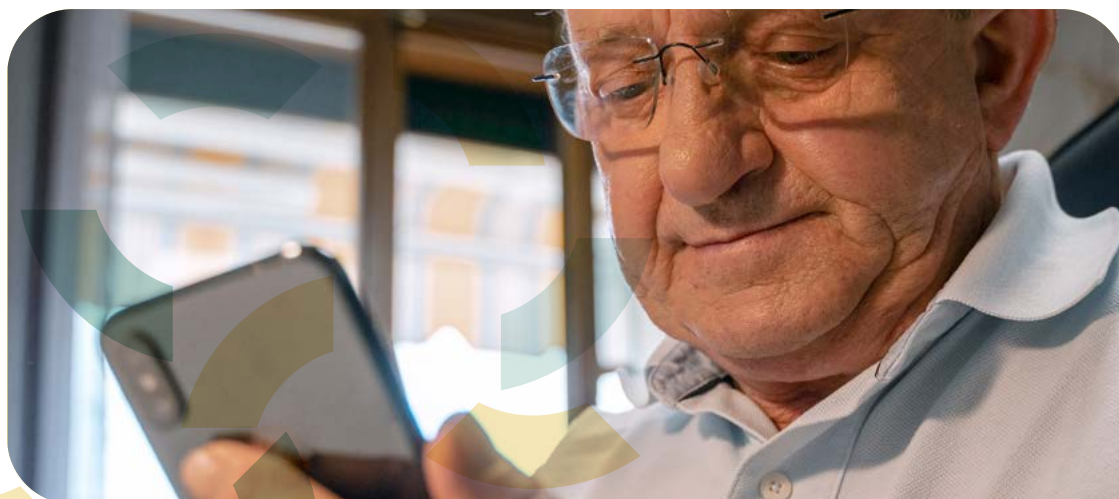
9. Deshabilita los complementos y permisos no deseados de los navegadores y aplicaciones instaladas en tu móvil

10. Borra tu historial de actividad digital para favorecer una navegación y búsquedas más privadas

2. Prevención de fraudes y estafas

No compartas datos personales o bancarios:

- Nunca envíes tu DNI, número de tarjeta, claves o códigos por WhatsApp, SMS, correo electrónico o llamadas, aunque parezca algo urgente o venga de alguien que conoces.
- Los bancos, la seguridad social o la policía nunca te pedirán tus datos por mensaje o llamada sin cita previa.



¿Qué es el phishing y cómo identificarlo?

El phishing es un engaño en el que alguien se hace pasar por una empresa conocida (banco, Amazon, Correos...) para robar tus datos.

Llega normalmente por correo, SMS o WhatsApp y te dice cosas como:

- “Tu cuenta ha sido bloqueada”
- “Falta un pago, haz clic aquí”
- “Actualiza tus datos urgentemente”



↑
ÍNDICE

Cómo reconocerlo:

- El mensaje tiene errores de ortografía o te produce presión o urgencia.
- El enlace parece raro o no es la web oficial.
- Te pide que introduzcas contraseñas o datos personales.



No hagas clic en los enlaces sospechosos. Borra el mensaje y consulta directamente con la empresa

¿Qué es un código QR?

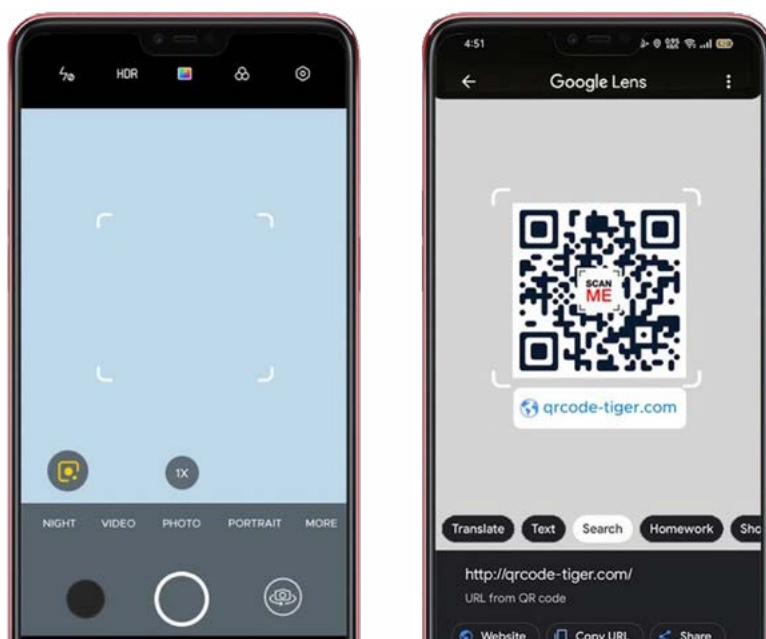
Un código QR es ese cuadrado de puntitos que puedes escanear con tu cámara. Pero también puede usarse para engañar. Los códigos QR (Quick Response) son códigos de barras, capaces de almacenar información variada. Gracias al auge de los nuevos teléfonos inteligentes o SmartPhone estos códigos QR están actualmente muy de moda, ya que es una forma de almacenar información y poder acceder a ella de manera rápida. El código QR está cada vez más presente en nuestras vidas y es el código bidimensional más popular del mundo.



↑
ÍNDICE

¿Cómo escanear un código QR?

Hay varias formas de hacerlo. Puedes usar la aplicación de la marca de tu móvil que viene instalada o Google Lens, que es la aplicación de Google y que también suele venir instalada para la lectura de Códigos QR de manera rápida y sin publicidad.



↑
ÍNDICE

1. Abre la aplicación de la cámara de su móvil.
2. Haz clic en el icono de Google Lens que verán la parte superior.
3. Posiciona el código QR dentro del recuadro blanco.
4. Pulsa en el texto azul que aparece para abrirlo.

Consejos:



**Solo escanea códigos QR de lugares confiables
(centros oficiales, restaurantes, carteles físicos)**

**Tras escanear, verifica que la web que aparece es
real y conocida**

¿Cómo reconozco comportamientos sospechosos?

Señales de alerta:

- Te escriben o llaman pidiéndote que envíes dinero urgente.
- Alguien te dice que ha cambiado su número y te pide un código.
- Te ofrecen un premio o regalo sin haber participado en nada.
- Aparecen mensajes que dicen: “Reenvía esto a 10 personas o se borrará tu cuenta”.

4. Protección frente a noticias falsas y desinformación

Cada vez circulan más noticias falsas, fotos manipuladas o vídeos falsos en redes sociales. Muchos de estos contenidos se crean usando herramientas de inteligencia artificial (IA), lo que los hace más difíciles de detectar y mucha gente los comparte sin saberlo. Esto puede causar miedo, confusión o engaños. Por eso, es importante conocer cómo identificarlos y qué hacer si los encontramos.

↑
ÍNDICE

Tipos de contenidos falsos o realizados con inteligencia artificial

- **Imágenes falsas generadas por IA:** Fotografías realistas que nunca ocurrieron (por ejemplo, una persona famosa en una situación comprometida o inventada).
- **Vídeos manipulados (deepface):** Vídeos en los que una persona, con una superposición de rostro, parece decir o hacer algo que nunca dijo o hizo. Suelen usarse para engañar o desprestigiar.
- **Audios falsos (deepvoice):** Grabaciones de voz creadas artificialmente que imitan el tono y acento de una persona para hacer creer que dijo algo que no es real.
- **Textos y noticias inventadas (fake news):** Noticias que parecen bien redactadas pero son completamente falsas. A veces se difunden con apariencia de noticia real en redes sociales o cadenas de WhatsApp.

¿Cómo identifico y verifico estos contenidos antes de compartirlos?

- **Antes de compartir, pregúntate: ¿Lo ha publicado una fuente confiable? ¿Es reciente o es algo viejo? ¿Quién lo ha escrito? ¿Otras páginas también lo dicen?**

- **Fíjate en los detalles visuales: En imágenes falsas generadas por IA, con formas extrañas, fondos borrosos o expresiones poco naturales**

- **Revisa la fuente: Si no proviene de un medio de comunicación conocido y contrastado, puede ser falso**

- **Sospecha si genera emociones fuertes: Los bulos suelen buscar provocar miedo, enfado o sorpresa. Si algo te parece demasiado exagerado o alarmante, desconfía**

- **Busca la información en otras fuentes: Si una noticia es real, aparecerá también en medios oficiales o en webs de verificación**

- **Observa el lenguaje: Si el texto tiene errores, mayúsculas por todas partes o frases confusas, puede ser una señal de que es un bulo**

↑
ÍNDICE

¿Qué hago si encuentro un contenido falso?

- Evita cadenas engañosas. No compartas información sin verificarla. Así evitas que el engaño llegue a más personas.
- Informa a quien haya compartido este tipo de información. Puedes decirle, con respeto, que es falsa.
- Denuncia este tipo de información en las redes sociales. Todas tienen opciones para marcar un contenido como engañoso o falso.
- Consulta gratuitamente estas webs de verificación y comprueba que la información que recibes es cierta:

↑
ÍNDICE



M MALDITA.ES

<https://maldita.es>



Newtral

<https://www.newtral.es>



Verifica**rtve**

<https://verifica.rtve.es>

Comparte información con prudencia

- No todo lo que circula por Internet es verdad, aunque parezca real. Sé consciente de lo que compartes y hazlo con prudencia

- Con pequeñas precauciones puedes protegerte de los engaños más comunes en Internet. Piensa con quién compartes y por qué motivo

- Recuerda que todo lo que compartes en Internet, en redes sociales o aplicaciones puede ser visto en el futuro por personas que no deseas

- Utiliza canales directos y/o cifrados, para compartir información personal y documentación sensible

↑
ÍNDICE



4. Seguridad en Internet y redes sociales

Internet es una herramienta muy útil para informarse, comunicarse o entretenerse, pero también puede tener riesgos. Por eso es importante aprender a navegar y comunicarse con seguridad.

4.1

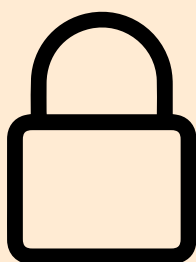
Navegación segura en Internet

1. Sitios web seguros

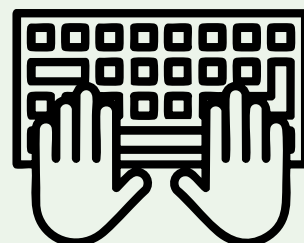
Antes de entrar a una página, verifica que sea segura:



El enlace debe empezar por "https://" (la "s" significa "seguro")



Aparece un candado al lado de la dirección web



Es mejor escribir tú mismo la dirección (por ejemplo: www.sepe.es) y no hacer clic en enlaces desconocidos



Evita páginas con muchos anuncios, avisos falsos o que piden tus datos sin explicación

2. Evita descargas peligrosas y enlaces sospechosos

Nunca descargues archivos de:

- Correos o mensajes de desconocidos

- Páginas que no conoces

- Enlaces acortados (como bit.ly) si no sabes a dónde llevan

- Si una página te ofrece descargar algo gratis o urgente, desconfía



Consejo:
Si dudas, pregunta antes a alguien de confianza



↑
ÍNDICE

4.2

Uso seguro de las redes sociales: Facebook e Instagram

Las redes sociales de Meta (Facebook e Instagram) son espacios muy populares para comunicarnos con la familia, amistades y personas con intereses similares. Usadas de manera segura, son una herramienta valiosa para mantenernos conectados, compartir recuerdos y estar al día.

Funciones principales y cómo usarlas:

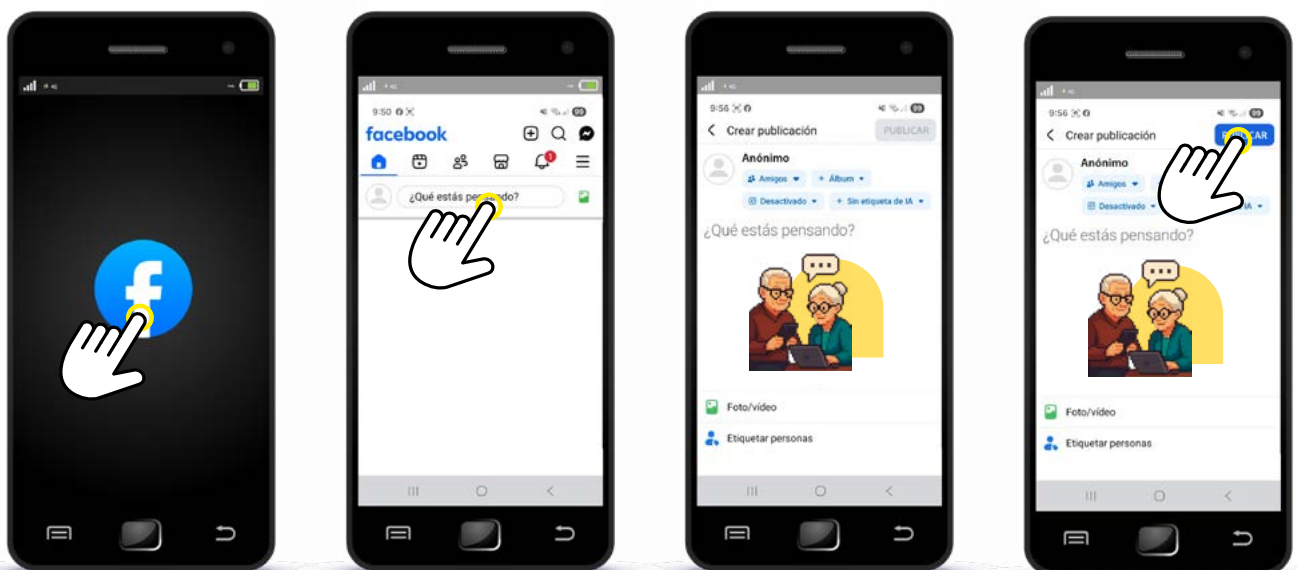
Facebook

- Publicar actualizaciones: escribir mensajes, compartir fotos o vídeos.
- Grupos y páginas: unirse a comunidades sobre temas de interés (manualidades, salud, historia).
- Eventos: confirmar asistencia a actividades culturales o charlas.
- Messenger: chatear de forma privada con contactos.

Paso a paso para publicar en Facebook:

1. Abre la aplicación de Facebook en tu móvil.
2. Pulsa en “¿Qué estás pensando?”.
3. Escribe tu mensaje o selecciona una foto.
4. Pulsa “Publicar”.

↑
ÍNDICE

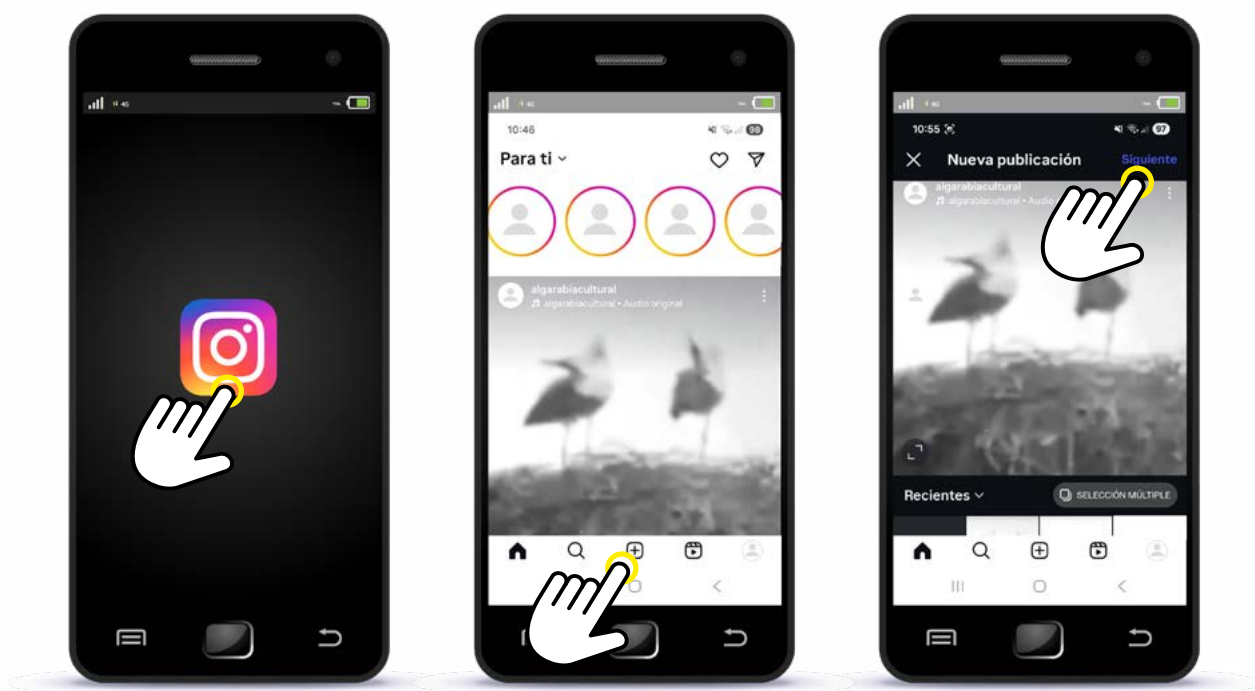


Instagram

- Publicar fotos o vídeos: mostrar momentos importantes.
- Historias: imágenes o vídeos breves que desaparecen en 24 horas.
- Seguir cuentas: ver publicaciones de amistades, familiares o temas que te interesen.
- Mensajes directos (DMs): enviar mensajes privados a contactos.

Paso a paso para publicar en Instagram:

1. Abre la aplicación de Instagram.
2. Pulsa el símbolo “+” en la parte inferior.
3. Elige una foto de tu galería o haz una nueva.
4. Opcional: añade un texto o emoticono.
5. Pulsa “Compartir”.



↑
ÍNDICE

Consejos para un uso seguro de Facebook e Instagram

1. Configura la privacidad de tu perfil

En redes como Facebook o Instagram, puedes decidir quién ve tus publicaciones:

1. En Facebook:
“Menú > Configuración > Privacidad”

En Instagram:
“Perfil > Menú (≡) > Configuración > Privacidad > Cuenta privada”

2. Elige que sólo tus amigos o contactos puedan ver tus fotos, publicaciones o información personal

3. No es necesario mostrar tu dirección, número de teléfono o lugar de trabajo

4. Revisa también quién puede enviarte solicitudes de amistad



ÍNDICE

2. No aceptes solicitudes de desconocidos

1. Si no conoces a la persona, no aceptes su solicitud de amistad

2. Puede tratarse de un perfil falso que quiere estafarte o acceder a tu información

3. No compartas tu número o fotos con personas que no conoces bien

3. Evita compartir la ubicación o tu información personal

1. No publiques cuándo estás de viaje o fuera de casa

2. Desactiva la ubicación en tiempo real en WhatsApp o redes sociales

3. Es mejor mantener en privado tus movimientos y datos personales

4. Cómo desactivar la ubicación



EN DISPOSITIVOS ANDROID

Opción rápida desde el menú rápido:

1. Desliza el dedo desde arriba de la pantalla hacia abajo para abrir el panel de accesos rápidos.
2. Busca el icono de ubicación 
3. Si está activado (de color), pulsa sobre él para desactivarlo (debería ponerse gris o apagarse).

Opción desde Ajustes:

1. Ve a la App de “Ajustes” (icono de rueda dentada ).
2. Toca en “Ubicación” o “Seguridad y ubicación”.
3. Pulsa el interruptor o botón que dice “Activado” y cámbialo a “Desactivado”.



EN DISPOSITIVOS IPHONE

1. Abre la App de “Configuración”.
2. Baja hasta “Privacidad y seguridad”.
3. Toca “Localización”.
4. Pulsa el botón de arriba para ponerlo en “No” y desactivarla.



ÍNDICE



4.3

Uso seguro de las aplicaciones de comunicación instantánea: conversaciones, videollamadas y reuniones en línea

Muchas de las aplicaciones que usamos hoy en día con nuestro dispositivo permiten comunicarnos de formas distintas con familiares, amistades o profesionales desde casa. Incluso nos permiten hacer videollamadas para hablar cara a cara. Por eso, se recomienda no entrar en enlaces de reuniones o videollamadas que te envíen personas desconocidas.

1. ¿Cómo usar WhatsApp de forma segura?

WhatsApp permite enviar mensajes, hacer llamadas, enviar fotos, vídeos, notas de voz y realizar videollamadas con tus contactos, sin costo adicional (solo necesitas conexión a Internet).

PRIMEROS PASOS

1. Descarga WhatsApp

- Abre la Play Store (en Android) o App Store (en iPhone).
- Escribe “WhatsApp” en el buscador.
- Pulsa “Instalar”.

2. Abre la aplicación y configúrala

• Toca el icono verde con un teléfono blanco

• Acepta los términos y condiciones



• Introduce tu número de teléfono móvil

• Recibirás un mensaje SMS con un código de verificación. Escríbelo

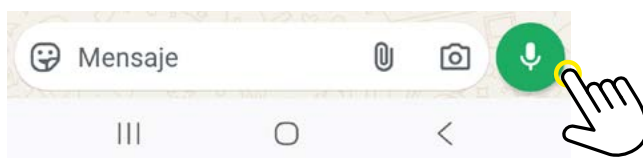
• Escribe tu nombre y, si quieres, añade una foto de perfil

FUNCIONES BÁSICAS

Envía un mensaje

1. Cuando abrimos WhatsApp, abajo a la derecha aparece este dibujo. Pulsa encima del icono de mensaje nuevo.
2. Aparecerá la lista de contactos de nuestro móvil que también tienen WhatsApp.
3. Elige un contacto de tu agenda. Busca a la persona con la que quieras hablar y pulsa encima del nombre.
4. Toca encima de mensaje para empezar a escribir y pulsa la flecha para enviar (flecha verde).

Envía una nota de voz



1. Usa el micro para mandar un mensaje de voz

2. Abajo a la derecha, en un círculo verde encontrarás el símbolo del micrófono

3. Déjalo pulsado para grabar y levanta el dedo para enviar

↑
ÍNDICE

Envía una foto o vídeo

1. Abre la conversación de la persona o grupo a la que quieras mandar una foto.
2. Pulsa el icono del clip  (o el icono de cámara .
3. Ahora pulsa el círculo morado Galería para enviar una foto o vídeo que ya tienes y toca sobre la foto o vídeo que quieras enviar.
4. Pulsa la Cámara para tomar una foto en ese momento.
5. Abajo a la derecha aparecerá una flecha para enviar.

Haz una llamada o videollamada

1. Entra en el chat de un contacto.
2. Pulsa el icono de teléfono para llamar.
3. Pulsa el icono de cámara para videollamada.

Añade un contacto con un chat nuevo



1. Ve a la pestaña Chats



2. Toca el icono de nuevo chat y después en “Nuevo contacto”

Añade un contacto desde un chat

1. Pulsa el chat de un número que no tengas guardado. Deberías ver un número de teléfono en lugar de un nombre.
2. Toca la parte superior del chat para ver la sección “Información del chat”.
3. Pulsa Guardar, ingresa los detalles y, luego, toca Guardar.

Fija conversaciones

1. Pulsa durante 2 segundos la conversación que quieras que siempre esté la primera, arriba aparecerán varios dibujos.
2. Pulsa la chincheta.
3. En iPhone, desliza hacia la derecha el chat que quieres fijar y luego presiona “Fijar”.
4. El máximo de conversaciones que se pueden fijar son 3.

Elimina conversación

1. Mantén presionado el chat y luego pulsa el icono de la papelera.
2. En iPhone, desliza hacia la derecha el chat que quieres eliminar y luego presiona “Eliminar”.

Crea un grupo de WhatsApp

1. Desde la ventana Chats, presiona los tres puntos ubicados en la parte superior derecha de la pantalla.
2. En el menú que te aparece, pulsa sobre Nuevo grupo.
3. Se abrirá el listado de tus contactos. Selecciona a aquellos contactos que quieres que estén en el grupo y pulsa sobre la flecha color verde (abajo derecha)

4. Presiona sobre el icono con forma de cámara para cargar una imagen que represente al grupo. Podrás subir una foto de la galería de tu móvil. Cuando la elijas, pulsa sobre y ella y después pulsa Ok.
5. Escribe el nombre que quieras ponerle al grupo sobre la palabra Asunto y presiona sobre el icono verde (Siguiente) para crearlo.
6. Si queremos un grupo donde sólo estemos nosotros, tenemos que abrir un grupo nuevo, al que añadiremos sólo a una persona de confianza. Una vez creado el grupo con esa persona, deberemos “Eliminar” del grupo a dicha persona. Para ello, pulsamos en el nombre del grupo, pinchamos encima del nombre de la persona a eliminar y la eliminamos. ¡Listo!, ya tenemos un espacio dentro de nuestro WhatsApp donde nadie más verá lo que enviamos.

Crea una comunidad de WhatsApp

1. Pulsa en la nueva pestaña de “Comunidades”.
2. Pulsa en la opción de “Iniciar una comunidad”.
3. Escribe el nombre y la descripción de la comunidad, añade una imagen. Esta información será visible para todos. Es importante que se entienda bien.
4. Crea un nuevo grupo o añade grupos ya existentes en los que seas administrador. Como máximo, 50 grupos.



ÍNDICE

Privacidad y seguridad en WhatsApp

• Solo tus contactos guardados pueden ver tu estado y foto de perfil (puedes cambiarlo en Ajustes > Privacidad)

• WhatsApp cifra todos los mensajes, lo que significa que solo tú y la otra persona pueden leerlos

• No compartas códigos, claves ni información personal por mensaje si no conoces bien al contacto

CONSEJOS PARA UN USO SEGURO

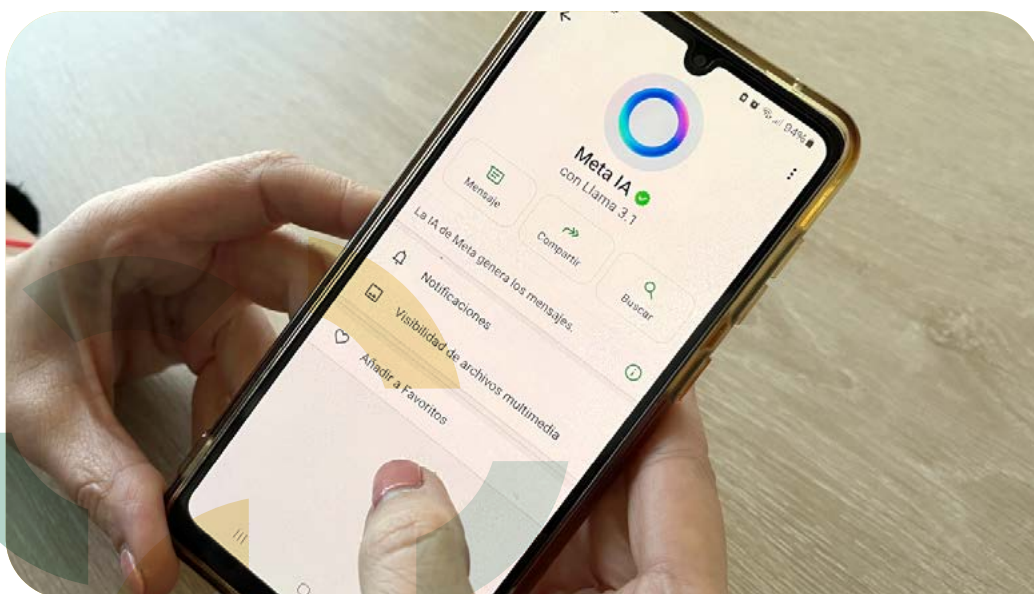
- No aceptes mensajes o llamadas de números desconocidos sin verificar.
- No compartas tu ubicación ni fotos privadas con personas que no conoces.
- Si alguien te molesta, puedes bloquear el contacto desde su perfil.
- Puedes hacer grupos de familia o amigos, pero siempre con personas de confianza.
- Si recibes mensajes desde números desconocidos, haciéndose pasar por algún conocido o familiar con algún problema o urgencia, comprueba por otra vía que se trata realmente de esa persona, antes de responder.

¿Qué es Meta IA en WhatsApp?

Meta IA es un asistente virtual o “chatbot” que WhatsApp ha integrado en la aplicación para ofrecer funciones extra basadas en inteligencia artificial. No es otro usuario, es una herramienta dentro de la aplicación que puedes usar para preguntar cosas, pedir ayuda, generar contenido y muchas más. No está disponible todavía en todos los dispositivos, ya que se está implementando de manera progresiva en todas las regiones. Algún día Meta IA te llegará y lo tendrás a tu disposición.



ÍNDICE



Funciones principales de Meta IA

Estas son algunas de las cosas que puedes hacer con la IA en WhatsApp:

Función	Qué hace	Ejemplo práctico
Chat con IA	Conversar con Meta IA, hacer preguntas sobre temas diversos: recetas, historia, traducciones, ayuda para tareas cotidianas	Preguntar “¿Cómo preparar arroz con pollo?” o “¿Cuál es la capital de Perú?”
Voz	En algunos dispositivos puedes hablar con Meta IA en vez de escribir	Decir “¿Qué tiempo hará mañana?” usando tu voz, como si fuese una llamada
Generación de contenido visual	Crear imágenes o fondos personalizados con descripciones escritas; por ejemplo, para usar como fondo de conversación	Escribir “puesta de sol sobre el mar” y que la IA genere una imagen para fondo de chat
Stickers creados por IA	Generar pegatinas (“stickers”) nuevos usando la IA, describiendo cómo los quieres	“Sticker de gato con sombrero” recibes ese sticker
Memoria / respuestas personalizadas	La IA puede recordar cosas que le digas para adaptar mejor sus respuestas, aunque esto tiene límites y configuraciones de privacidad	
Ayudas prácticas	Traducciones, resumir textos largos, sugerir respuestas, ideas de mensajes	

↑
ÍNDICE



Aspectos a tener en cuenta para usar Meta IA con seguridad

Para que la IA te sea útil y no te cause preocupaciones, conviene que tengas en cuenta que:

- Meta IA es opcional y no es obligatorio usarla.
- La IA sólo tiene acceso a lo que le envías directamente; no “lee” tus otras conversaciones sin que tú lo autorices.
- Las respuestas pueden no ser siempre exactas, correctas o completas. Te recomendamos comprobar y comparar con otras fuentes si vas a tomar decisiones importantes.
- Revisa los ajustes de privacidad: qué datos permites que la IA “recuerde”, qué información personal compartes, siempre con precaución.
- Mantén la aplicación actualizada, para tener los últimos parches de seguridad y las últimas mejoras.

2. ¿Cómo usar Zoom de forma segura?

↑
ÍNDICE



Zoom es una aplicación que te permite hacer videollamadas con una o varias personas al mismo tiempo. Es ideal para hablar con la familia, asistir a clases o reuniones sin salir de casa.

OPCIÓN 1: USAR ZOOM EN EL MÓVIL O TABLET (Android o iPhone)

1. Descarga la aplicación Zoom

- Abre la Play Store (Android) o App Store (iPhone).
- Busca: “Zoom Cloud Meetings”.
- Pulsa “Instalar”.

2. Abre la aplicación

- Toca el icono de Zoom (una cámara blanca sobre fondo azul).

3. Únete a una reunión

- Pulsa “Unirse a una reunión”.
- Escribe el ID de la reunión que te han enviado (un número de 9 a 11 dígitos).
- Escribe tu nombre.
- Pulsa “Unirse”.
- Si te lo piden, introduce la contraseña de la reunión.

4. Acepta el permiso para usar el Micrófono y la Cámara

- Pulsa “Permitir” en ambos casos para que te escuchen y te vean.

OPCIÓN 2: USAR ZOOM EN EL ORDENADOR (Windows o Mac)

1. Abre el navegador (Chrome, Firefox, etc.)

- Escribe: www.zoom.us

2. Únete a una reunión

- Haz clic en “Unirse a una reunión” (parte superior derecha).
 - Escribe el ID de la reunión y pulsa Entrar.
 - Si no tienes Zoom instalado, el navegador te ofrecerá descargarlo. Haz clic en “Descargar e instalar” y sigue las instrucciones.
- ### 3. Acepta y permite los permisos de uso del micrófono y cámara si te lo pide el sistema.

↑
ÍNDICE

CONSEJOS PARA USAR ZOOM CON SEGURIDAD

• Activa solo tu cámara y micrófono si te sientes cómodo/a

• Si hay ruido de fondo, pulsa el botón del micrófono para silenciarte

• Si quieres hablar, pulsa el micrófono de nuevo para activar el audio

• No compartas el enlace de la reunión con personas que no conozcas

3. ¿Cómo usar Google Meet de forma segura?

Google Meet es una aplicación gratuita de videollamadas que puedes usar desde tu móvil, tableta u ordenador. Sólo necesitas conexión a Internet y una cuenta de correo de Gmail (como tunombre@gmail.com). Asegúrate de que el enlace sea oficial (empieza por <https://meet.google.com/>).



OPCIÓN 1: USA GOOGLE MEET EN EL MÓVIL O TABLET

1. Descarga la aplicación

- Abre la Play Store (Android) o App Store (iPhone).
- Busca: Google Meet.
- Pulsa “Instalar”.

2. Abre la App

- Pulsa en el icono de Google Meet (una cámara de colores sobre fondo blanco).
- Inicia sesión con tu cuenta de Google (Gmail) si te lo pide.

3. Únete a una reunión

- Toca el botón “Unirse con un código”.
- Escribe el código o enlace que te han enviado por correo o WhatsApp (por ejemplo: abc-defg-hij).
- Pulsa “Unirse”.

4. Permite el acceso a la cámara y el micrófono cuando el dispositivo te lo solicite.



ÍNDICE

OPCIÓN 2: USAR GOOGLE MEET EN EL ORDENADOR

1. Abre tu navegador (Chrome o Firefox)

- Ve a <https://meet.google.com>

2. Inicia sesión con tu cuenta de Gmail

- Si no tienes una sesión iniciada, te pedirá tu dirección de correo y contraseña.

3. Únete a una reunión

- Haz clic en “Unirse a una reunión”.
- Escribe el código o enlace de la videollamada.
- Pulsa “Unirse”.
- El navegador te pedirá permiso para usar la cámara y el micrófono. Haz clic en “Permitir”.

CONSEJOS PARA UN USO SEGURO

- **Entra sólo a reuniones con personas de confianza**

- **No compartas el enlace de la reunión con desconocidos.**

- **Si no quieres que te vean, puedes apagar la cámara.**

- **Si hay mucho ruido, puedes silenciar tu micrófono.**

- **Usa auriculares si estás en un lugar público.**

- **Evita mostrar información personal o tu casa en la cámara.**

↑
ÍNDICE

Con estas buenas prácticas, puedes usar Internet, las redes sociales y hacer videollamadas de forma segura y tranquila. Aprender a protegerte es tan importante como aprender a comunicarte. Recuerda que todas estas aplicaciones están sujetas a condiciones de uso y debes aceptar los permisos para poder usarlas.

5. Trámites y compras por Internet

Internet nos permite hacer compras y trámites desde casa, ahorrando tiempo y evitando esperas. Este apartado te enseñará a usar Internet de forma segura para tus gestiones personales, ayudándote a identificar engaños y protegerte mientras navegas y compras por internet.

5.1 Certificado digital

1. ¿Qué es el Certificado Digital?

El certificado digital es como tu DNI electrónico en el ordenador o en el móvil. Es un archivo que confirma tu identidad cuando haces trámites por Internet con la Administración Pública u otras entidades oficiales. Es personal e intransferible, y te permite firmar y validar documentos como si estuvieras allí en persona.

2. ¿Para qué sirve?

Con el certificado digital puedes hacer gestiones desde casa, como por ejemplo:

- Solicitar la vida laboral o la pensión

- Presentar la declaración de la renta

- Consultar datos médicos

- Pagar impuestos o multas

- Obtener certificados de nacimiento, empadronamiento, etc.

3. ¿Qué ventajas tiene?

- Seguridad: garantizas que solo tú accedes a tus datos y documentos.
- Comodidad: puedes hacer trámites desde casa, sin colas ni papeleo.
- Validez legal: tiene el mismo valor que una firma presencial.
- Ahorro de tiempo y desplazamientos.

4. ¿Cómo puedo instalarlo?

PASO 1: SOLICÍTALO

- Ve a la web oficial de la Fábrica Nacional de Moneda y Timbre (FNMT): <https://www.sede.fnmt.gob.es>
- Solicita tu certificado de persona física.
- Introduce tus datos y recibirás un código por correo electrónico.

En el siguiente video tutorial la Agencia Tributaria te explica paso a paso como solicitar el certificado digital:



↑
ÍNDICE

PASO 2: VERIFICA TU IDENTIDAD

- Debes ir presencialmente a un punto de registro autorizado (como una oficina de Hacienda o Seguridad Social) con tu DNI y el código que recibiste.
- Puedes ir acompañado/a por un familiar si lo necesitas.

PASO 3: DESCÁRGALO E INSTÁLALO

- Después de verificar tu identidad, volverás a la web de la FNMT.
- Introduce tu DNI y el código.
- Descarga el certificado e instálalo en tu navegador (como Chrome o Firefox).
- También puedes exportarlo a un USB o instalarlo en el móvil.

5.2

Cómo pido una cita previa de forma segura

Hoy en día, muchos trámites requieren cita previa online: médico, DNI, Seguridad Social, Hacienda, etc. Hacerlo tú mismo desde casa es posible y seguro si sabes cómo reconocer los sitios oficiales.

1. ¿Cómo identifico una web oficial?

A continuación, se muestran las características de una web oficial y segura:

Elemento

Cómo saber si es oficial

Dirección web (URL)

Termina en .gob.es o .org (ejemplo: www.seg-social.gob.es)

Candado

Aparece al lado de la dirección, indica conexión segura

Diseño

Profesional, sin anuncios ni ventanas emergentes raras

No piden dinero

Salvo en trámites concretos y claros como tasas oficiales



Evita páginas que digan “cita rápida” o “gestión urgente” si no son del gobierno. Muchas cobran por un servicio gratuito

2. Sitios seguros para trámites frecuentes

Trámite	Dirección web
Cita médica (Andalucía)	https://www.sspa.juntadeandalucia.es/servicioandaluzdesalud o usa la App Salud Responde
DNI / Pasaporte	https://www.citapreviadnie.es
Agencia Tributaria	https://www.agenciatributaria.gob.es
Seguridad Social	https://www.seg-social.gob.es

3. ¿Qué fraudes comunes tienes que evitar?

- Páginas que te cobran por conseguirte la cita.
- Sitios que te pidan el número de cuenta bancaria sin motivo.
- Enlaces que te lleguen por WhatsApp o correo y no sabes quién los envía.
- Nunca des tu número de cuenta, tu PIN o tu contraseña.

↑
ÍNDICE



4. ¿Cómo pido una cita?

1. Entra en la web oficial del organismo (o en su aplicación si la tiene)

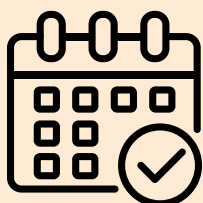
2. Busca el botón que diga “Cita previa”

3. Elige el tipo de trámite (por ejemplo: renovación DNI, consulta médica)

4. Rellena tus datos personales (nombre, DNI, teléfono)

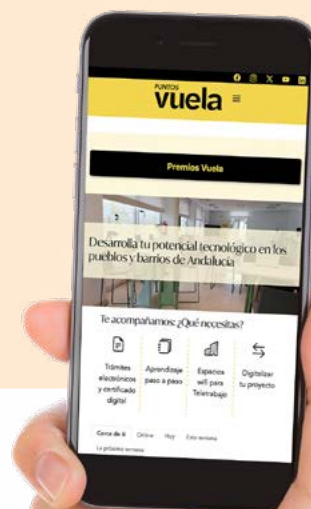
5. Elige la fecha y la hora

6. Guarda el comprobante o haz una captura de pantalla



Pedir cita previa por Internet es una buena forma de ganar autonomía, siempre que lo hagas en sitios oficiales. Si una web no te da confianza, es mejor salir y preguntar

Si tienes alguna duda, puedes acudir a tu Punto Vuela más cercano



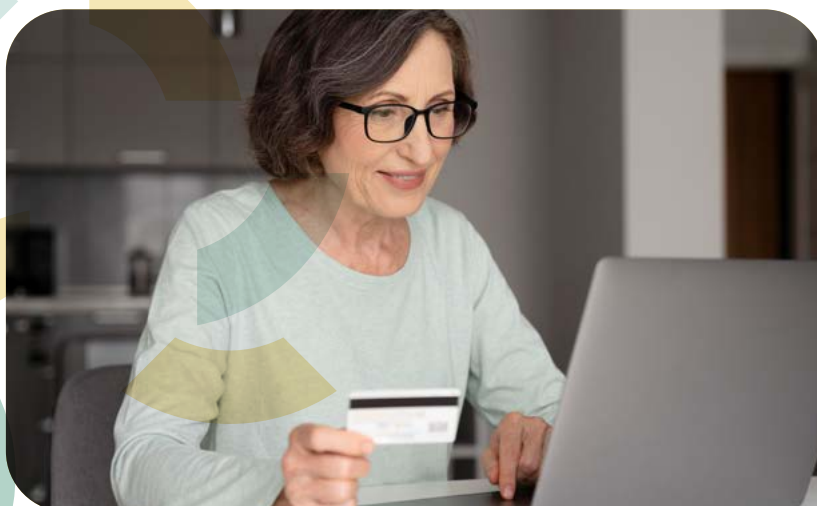
5.3 Compras Online

Comprar por Internet te permite recibir productos en casa sin desplazarte. Pero es importante seguir unas precauciones básicas para no caer en fraudes ni estafas.

1. Recomendaciones para comprar de forma segura

Haz esto	Evita esto
Compra en tiendas conocidas (El Corte Inglés, Amazon, Carrefour, etc.)	Sitios con ofertas demasiado buenas o sin información clara
Revisa que la web comience por https:// y tenga un candado	Webs que solo dicen “http” (sin “s”)
Lee opiniones de otros compradores	Páginas sin reseñas ni datos de contacto
Guarda un comprobante de la compra	Comprar sin recibir confirmación ni factura
Revisa las condiciones de devolución	Comprar sin saber si puedes devolver el producto

↑
ÍNDICE



2. ¿Cómo pago con seguridad?

Existen varias formas seguras de pagar por Internet. Aquí te explicamos las tres más comunes:

¿Cómo pago por Internet con tarjeta de crédito, débito o prepago?

1. Entra en una página web segura (con https:// y candado .
2. Elige el producto o servicio que quieres comprar.
3. En el momento del pago, selecciona “Tarjeta”.
4. Introduce los datos de la tarjeta:



5. Confirma el pago (normalmente con un código que llega por SMS o por la app del banco).

¿Qué es una tarjeta prepago?

Una tarjeta prepago es una tarjeta para pagar por Internet (y en tiendas) que solo tiene el dinero que tú decides cargarle previamente. No está vinculada directamente a tu cuenta bancaria principal, por lo que ofrece más control y seguridad.

¿Por qué es una buena opción para pagar por internet?

Las tarjetas prepago son especialmente recomendables para las personas mayores, ya que nos aportan tranquilidad y confianza al comprar Online. Porque limitan el riesgo en caso de fraude, nos ayudan a controlar mejor los gastos y son ideales para hacer compras puntuales o en páginas webs menos habituales.

¿Cómo consigo una tarjeta prepago?

Podemos obtenerla a través de nuestra entidad bancaria, de manera física o virtual, aunque no todas cuentan con este servicio, tendremos que informarnos primero. Una vez tengamos la tarjeta de prepago, podremos recargarla desde nuestra cuenta bancaria, desde un cajero o a través de la app de nuestro banco. Cuando tengamos saldo en la tarjeta, la podremos utilizar para realizar nuestras compras por Internet como si fuera una tarjeta de crédito o débito.



PayPal actúa como una barrera de seguridad entre tu tarjeta y la tienda. No compartes tus datos bancarios con el vendedor.

Cómo usar PayPal:

1. Ve a www.paypal.es y crea una cuenta.
2. Añade tu tarjeta de crédito o débito una sola vez.
3. Cuando compres online, selecciona “Pagar con PayPal”.
4. Inicia sesión en PayPal y confirma el pago.



Si hay un problema con la compra, PayPal puede ayudarte a recuperar tu dinero

↑
ÍNDICE



Bizum es un sistema para enviar dinero entre móviles o pagar en tiendas online, sin necesidad de dar tu número de cuenta.

Cómo usar Bizum:

1. Debes activarlo desde la App de tu banco.
2. Cuando compres en una tienda online compatible, selecciona “Pagar con Bizum”.
3. Introduce tu número de teléfono y el código Bizum (lo da tu banco).
4. Confirma la compra con un mensaje o notificación en tu móvil.



Solo funciona si tienes activado Bizum desde tu banco. Es rápido y seguro

Consejos para comprar y pagar con seguridad en internet

- Compra en tiendas conocidas o de confianza

- Verifica que la web sea segura (https y candado )

- Usa métodos seguros de pago: Bizum, PayPal o tarjeta bancaria

- No compartas tus datos personales o bancarios por mensaje

- Guarda siempre el comprobante de la compra

- Evita comprar desde conexiones a redes Wi-Fi públicas



ÍNDICE



6. Uso responsable del correo electrónico

El correo electrónico es una herramienta esencial para comunicarnos y gestionar trámites, pero también un canal para fraudes. Este apartado te enseñará a identificar correos sospechosos, proteger tus datos y usar tu correo de forma segura y confiable.

6.1

¿Qué es un correo electrónico y cómo funciona?

Un correo electrónico (email) es como una carta digital que puedes enviar a otra persona usando Internet. En lugar de ir al buzón, el mensaje llega a un buzón virtual que puedes ver desde tu móvil, tableta o PC. Es útil para comunicarte y enviar documentos, pero cada vez más necesario para recibir avisos del médico y hacer trámites bancarios u oficiales.

↑
ÍNDICE

1. ¿Cómo creo una cuenta de correo electrónico?

Una cuenta de correo electrónico te permite recibir mensajes, hacer gestiones online y registrarte en servicios digitales. Pero es importante hacerlo con seguridad desde el principio.

PASOS PARA CREAR UNA CUENTA EN GMAIL (Google)
(muy similar en Outlook, Yahoo u otros servicios)

1. Abre el navegador (Chrome, Firefox...) y entra en www.gmail.com
2. Pulsa “Crear cuenta”.
3. Escribe tu nombre y apellidos.
4. Elige un nombre de usuario (por ejemplo: carmen.gomez1952@gmail.com).
5. Crea una contraseña segura, combinando letras en mayúscula, números y símbolos. Anótala para que no se te olvide.
6. Añade tu número de teléfono y una dirección de correo de recuperación (opcional, pero útil).
7. Acepta las condiciones y pulsa “Siguiente”.

2. ¿Cómo envío un correo electrónico?

Aquí tienes el paso a paso básico usando Gmail (muy similar en Outlook, Yahoo u otros servicios):

PASOS DESDE UN TELÉFONO O PC

1. Abre la App de Gmail o entra en www.gmail.com

- Inicia sesión con tu cuenta de correo y tu contraseña.

2. Pulsa “Redactar” o “Escribir”

- Aparece como un botón con un lápiz o símbolo 

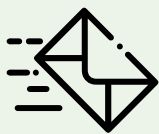
3. Completa los campos del mensaje:

- Para: escribe la dirección de la persona a quien quieres enviar el mensaje (ejemplo: pepita77@gmail.com)
- Asunto: una frase breve que diga de qué trata el mensaje (ejemplo: “Cita médica del lunes”)
- Mensaje: escribe lo que quieres decir. Ejemplo: Hola Pepita, te escribo para confirmar que el lunes a las 10:30 estaré en el centro de salud.

4. (Opcional) Adjuntar un archivo o foto

- Pulsa el icono de clip o imagen para adjuntar documentos o fotos.

5. Pulsa “Enviar” (icono de flecha )



¡Y listo!

El mensaje llegará en pocos segundos



ÍNDICE

3. Consejos prácticos para organizar tu correo electrónico con seguridad

1. Lee y borra lo que no necesitas

Cada día o semana, entra a tu correo y borra los mensajes antiguos, promociones o avisos sin importancia.

Pulsa en el icono de papelera para eliminarlos.

2. Crea carpetas o etiquetas

En Gmail se llaman etiquetas, en Outlook se llaman carpetas.

Puedes crear categorías como:



Así podrás mover los correos importantes a su lugar y encontrarlos fácilmente.

3. Date de baja de correos molestos

Si recibes muchos correos de tiendas o boletines, pulsa en “Cancelar suscripción” o “Darse de baja” (normalmente está al final del correo).

Esto ayuda a reducir el ruido en tu bandeja.

4. Usa la lupa para buscar correos

En la parte superior, hay una barra de búsqueda donde puedes escribir palabras clave: “Pensión”, “recibo”, “Pepita”, “Seguridad Social”...

5. Archiva correos en lugar de borrarlos

Si no quieres borrar un mensaje pero ya lo leíste, puedes archivarlo para que no estorbe en la bandeja.

En Gmail, pulsa el icono de caja con flecha hacia abajo.

↑
ÍNDICE

RESUMEN

Qué hacer	Por qué hacerlo
Crear una contraseña fuerte	Para proteger tu cuenta
Borrar correos innecesarios	Para ver solo lo importante
Usar carpetas/etiquetas	Para encontrar todo más rápido
Darse de baja de publicidad	Para evitar correos molestos
Buscar con la lupa	Para no perder tiempo buscando

CONSEJOS DE SEGURIDAD

↑
ÍNDICE



Solo abre correos de personas o instituciones que conozcas



Desconfía de mensajes con premios, urgencias o enlaces extraños



Nunca compartas contraseñas o datos personales por correo



Revisa el remitente antes de abrir archivos adjuntos

6.2

Detecta correos sospechosos o fraudulentos

Al igual que en la vida real pueden llegar cartas falsas o engañosas, también ocurre con los correos electrónicos. Aprender a identificarlos es clave para proteger tu información y evitar estafas.

SEÑALES COMUNES DE UN CORREO FRAUDULENTO

RESUMEN

Señal de alerta	¿Qué significa?
Mensajes urgentes o con amenazas	“Si no respondes hoy, te cerramos la cuenta”
Ofertas increíbles o sorteos falsos	“Has ganado un iPhone, haz clic aquí”
Remitente extraño o desconocido	Direcciones raras: correo@segurid4dbanco.xyz
Enlaces o botones sospechosos	Enlaces que no llevan a sitios oficiales
Faltas de ortografía o frases mal escritas	“Tu cuenta esta en riesgo. Click aquí inmediato.”
Archivos adjuntos sin explicación	Documentos que pueden contener virus

↑
ÍNDICE

1. ¿Qué debes revisar antes de abrir un correo?

1. ¿Conoces a la persona o entidad que me escribe?

- Si no, no abras el mensaje ni descargues nada.
- Si te dice ser tu banco o la Seguridad Social, verifica que la dirección sea oficial (termina en .gob.es, .org, .es, etc.).

2. ¿Te piden datos personales o bancarios?

- Nunca des tu número de cuenta, contraseña, DNI o PIN por correo.
- Las entidades serias no piden información confidencial por email.

3. ¿El mensaje te mete prisa?

- “Tu cuenta ha sido bloqueada”
- “Haz clic ahora o perderás el acceso”



Esa urgencia suele ser una trampa para que no pienses



ÍNDICE

2. ¿Qué hacer si recibes un correo fraudulento?

- No abras los enlaces ni descargues archivos.
- Elimínalo directamente o márcalo como “correo no deseado” o “spam”.
- Si ya hiciste clic, cambia tus contraseñas y contacta con tu banco de inmediato.





DIFERENCIAS ENTRE PHISHING Y SPAM

	Phishing	Spam
Intención	Robarte datos personales o dinero	Enviarte publicidad o mensajes masivos
Peligro	Alto: puede provocar fraudes	Bajo, pero puede ser molesto
Apariencia	Se hace pasar por tu banco, una empresa o instituciones conocidas	Publicidad genérica, sin personalizar
Acción recomendada	Eliminar sin hacer clic y reportar	Marcar como spam y eliminar

↑
ÍNDICE

Como hemos visto en este apartado, el correo electrónico es una herramienta muy útil para comunicarnos, recibir información importante y realizar gestiones. Sin embargo, también presenta riesgos si no lo usamos con precaución. Con las indicaciones anteriores, protegemos nuestra información personal y evitamos caer en fraudes digitales. Así, el correo electrónico se convierte en un aliado para nuestra comunicación y no en un motivo de preocupación. La seguridad digital está en nuestras manos y cuanto más cuidemos nuestros hábitos digitales, más podremos disfrutar de la tecnología con confianza y tranquilidad.

7. Qué hacer si tengo un problema

Si te han engañado por internet, no es tu culpa. Actúa rápido para que el daño sea el menor posible.

7.1

Concepto de identidad digital y cómo protegerla

1. ¿Qué es la Identidad Digital?

La identidad digital es nuestra huella personal en la red. Es el conjunto de datos, imágenes, opiniones y rastros que dejamos en Internet sobre nosotros mismos.



ÍNDICE

Tu identidad digital incluye:

- Tu nombre y apellidos.
- Tu correo electrónico.
- Fotos y vídeos que publicas.
- Comentarios en redes sociales.
- Datos bancarios o sanitarios.
- Lo que otros publican sobre ti.

2. ¿Por qué es importante que la protejas?

Porque si no cuidas tu identidad digital:

- Otras personas pueden suplantarte.
- Pueden robarte información personal o bancaria.
- Pueden difundir fotos sin tu permiso.
- Puede dañar tu reputación o causar problemas legales.

3. ¿Cómo protejo mi Identidad Digital?

Aquí tienes 7 pasos sencillos y prácticos:

1. Usa contraseñas seguras y diferentes para cada cuenta.

- Combina letras mayúsculas, minúsculas, números y símbolos.
- Ejemplo: Verano2024!Salud

2. Activa la verificación en dos pasos.

- Así, además de la contraseña, tendrás un código de seguridad en tu móvil.
- Muy importante en correo electrónico y banca online.

3. Revisa la privacidad de tus redes sociales.

- En Facebook, Instagram o WhatsApp, configura que sólo tus amigos puedan ver tus publicaciones y datos.
- Evita publicar tu dirección o teléfono.

4. Piensa antes de publicar.

- ¿Te gustaría que esa foto o comentario lo vea cualquiera?
- Si no es necesario, no lo compartas.

5. Comprueba si aparece información tuya en Internet.

- Busca tu nombre en Google de vez en cuando.
- Si hay algo que no quieres que aparezca, puedes pedir que lo retiren.

6. Evita conectarte en redes Wi-Fi públicas para gestiones sensibles.

- No hagas operaciones bancarias ni compres online desde redes abiertas (cafeterías, aeropuertos).

7. Sospecha de mensajes que piden tus datos.

- Bancos, Seguridad Social y organismos oficiales nunca te pedirán contraseñas por correo o WhatsApp.



ÍNDICE

1. Detén el contacto con el estafador

- No respondas más mensajes, correos o llamadas.
- Bloquea el número o dirección de correo si puedes.

2. Cambia inmediatamente tus contraseñas

- Si diste datos de acceso (correo, banca online, redes sociales):
- Cambia la contraseña en ese servicio y en otros donde uses la misma clave.
- Usa una contraseña nueva y segura (combina letras, números y símbolos).

3. Contacta con tu banco si facilitaste datos bancarios, tarjetas o hiciste un pago:

- Llama enseguida a tu banco y explícale lo ocurrido.
- Pide que bloqueen la tarjeta si es necesario.
- Solicita información sobre si pueden devolver el pago o cancelar operaciones.

4. Guarda todas las pruebas, esto es importante para denunciar y demostrar lo ocurrido

- Capturas de pantalla de mensajes, correos, anuncios.
- Recibos de pagos o transferencias.
- Conversaciones con el estafador.



5. Denuncia la estafa. Cuando vayas a denunciar, lleva todas las pruebas que guardaste

Puedes denunciar de varias formas:

- Policía Nacional o Guardia Civil (presencialmente en comisaría o cuartel).
- Por Internet en: <https://www.osi.es/es/reporte-de-fraude> (Oficina de Seguridad del Internauta).
- Teléfono de ayuda al ciudadano en ciberseguridad INCIBE: 017 (gratuito y confidencial).



↑
ÍNDICE

6. Informa a familiares y personas de confianza

- Si has compartido información sensible, cuéntaselo a alguien de confianza.
- Si se trataba de tus redes sociales, avisa a tus contactos de que pueden recibir mensajes falsos de tu cuenta.

7. Aprende de la experiencia y revisa tu seguridad

- Revisa bien qué ocurrió para evitar que se repita.
- Activa la verificación en dos pasos en tus cuentas.
- Instala antivirus y actualiza tu dispositivo.
- Desconfía de mensajes que pidan dinero o datos con urgencia.

7.3

¿Qué hacer si han suplantado mi identidad?

La suplantación de identidad ocurre cuando alguien utiliza tus datos, tu nombre o tus fotos sin tu autorización para engañar, estafar o perjudicarte. Si te ocurre, actúa rápido para protegerte y evitar daños mayores.

1. No entres en pánico

- Es normal sentir nervios o preocupación.
- Tómate un momento para pensar con claridad.
- Recuerda: tienes derecho a denunciar y pedir ayuda.

2. Recoge todas las pruebas y guarda todo lo que demuestre que alguien se hace pasar por ti:

- Capturas de pantalla del perfil falso o mensajes.
- Enlaces web o direcciones de correo.
- Conversaciones donde otras personas confirman que han recibido mensajes falsos.
- Anota la fecha y hora en que descubriste la suplantación.



ÍNDICE



3. Cambia tus contraseñas de inmediato si sospechas que te han robado el acceso a alguna cuenta (correo, redes sociales, banca online):

- Cambia la contraseña por otra más segura.
- Activa la verificación en dos pasos si tu servicio lo permite (recibirás un código en el móvil cada vez que entres).
- Revisa si hay actividad sospechosa (por ejemplo, mensajes enviados sin tu permiso).

4. Informa a la plataforma o servicio si la suplantación ocurre en redes sociales:



Facebook:

- Entra al perfil falso.
- Pulsa los tres puntos (...) > “Denunciar”.
- Selecciona “Suplantación de identidad”.



Instagram:

- Abre el perfil falso.
- Pulsa (...) > “Denunciar”.
- Elige “Es contenido inapropiado” > “Suplantación de identidad”.



WhatsApp:

- Si alguien usa tu foto o tu nombre, avisa a tus contactos.
- Contacta con WhatsApp en support@whatsapp.com.

↑
ÍNDICE

5. Denuncia ante la Policía o Guardia Civil.

La suplantación de identidad es un delito. Puedes denunciar:

- De forma presencial en comisaría o cuartel.
- Aportando todas las pruebas recogidas.
- Puedes contar con un familiar o persona de confianza que te acompañe.

6. Informa a tus contactos para evitar confusiones y posibles estafas:

- Avisa a tus amigos, familia o compañeros que no respondan a mensajes sospechosos enviados en tu nombre.
- Pídeles que te avisen si reciben algo raro.

7. Refuerza tu seguridad digital

- Usa contraseñas únicas y seguras.
- Activa verificación en dos pasos.
- Revisa periódicamente tus cuentas y dispositivos.
- No publiques datos sensibles (DNI, dirección, teléfono) en redes públicas.



ÍNDICE

8. Inteligencia Artificial para un envejecimiento activo seguro

Según la Organización Mundial de la Salud (OMS), las personas mayores padecemos el 12,5% de todos los problemas de salud, física y mental, en todo el mundo. En este contexto las herramientas basadas en Inteligencia Artificial (IA) pueden ayudarnos a superar o reducir los obstáculos que existen ofreciéndonos nuevas formas de diagnóstico, tratamiento y seguimiento. A continuación proponemos algunas aplicaciones de utilidad para mejorar la salud física y mental de las personas mayores.



↑
ÍNDICE

8.1

Configura de forma segura el Asistente Virtual de tu móvil: Google

El Asistente de Google es un ayudante virtual que responde a tus preguntas, te recuerda tareas y controla aplicaciones con la voz. Para que sea útil y seguro, conviene revisar la configuración.

1. Activa y personaliza el Asistente

- Abre la App de Google en tu móvil.
- Pulsa tu foto de perfil (arriba a la derecha) > Ajustes > Asistente de Google.
- Entra en General y activa o desactiva el asistente según tu preferencia.
- Si lo quieres activo, configura tu voz con “Voice Match”, para que solo responda a ti.

2. Revisa la privacidad

En el menú de ajustes encontrarás “Privacidad”. Allí puedes:

- Borrar el historial de voz (lo que el asistente ha grabado).
- Activar la opción para que no se guarden grabaciones automáticamente.
- Revisar qué datos se usan para personalizar respuestas.

Paso a paso:

1. Abre Asistente de Google > Privacidad.
2. Pulsa “Actividad de voz y audio”.
3. Selecciona “Eliminar automáticamente cada 3 meses”.



ÍNDICE

3. Configura la seguridad en compras y pagos

El Asistente de Google puede hacer compras online o pagar en tiendas. Para mayor seguridad:

- Desactiva esta opción si no la usas.
- Si la usas, pide que solicite huella, PIN o reconocimiento facial antes de autorizar pagos. En Ajustes > Asistente de Google > Pagos.

4. Controla las notificaciones y accesos

- Decide qué aplicaciones puede abrir el Asistente (ejemplo: WhatsApp, Calendario).
- Desactiva accesos que no necesites.
- Revisa permisos en Ajustes del móvil > Aplicaciones > Asistente de Google > Permisos.

5. Uso responsable en el día a día

- No dictes al Asistente datos muy sensibles (números de tarjeta, claves, DNI).
- Cuando no lo uses, puedes desactivar el micrófono o quitar la activación por voz (“Ok Google”).
- Mantén la App siempre actualizada para mejorar seguridad.

↑
ÍNDICE



8.2

Configura de forma segura un Asistente Virtual en casa

Usar un asistente virtual de forma segura es importante, ya que este tipo de dispositivos pueden recopilar información personal y, si no los configuramos bien, pueden causarnos problemas y ser un riesgo importante para nuestra privacidad. A continuación, vamos a explicar cómo configurar Alexa (Amazon), ya que es el asistente virtual más conocido e implantado en los programas de atención y acompañamiento de personas mayores.

1. Instala Alexa de forma segura

1. Conecta el dispositivo Echo (el altavoz con Alexa) a la corriente.
2. Descarga la aplicación Amazon Alexa en tu móvil desde la Play Store (Android) o App Store (iPhone).
3. Abre la aplicación y sigue las instrucciones para conectar tu dispositivo a la Wi-Fi de casa (mejor no usar redes públicas).

2. Ajusta la seguridad y privacidad de Alexa

• Protege tu cuenta de Amazon

1. Activa la verificación en dos pasos en tu cuenta de Amazon (te pedirá un código adicional al iniciar sesión).
2. Usa una contraseña fuerte y única.

• Controla lo que Alexa escucha

1. Puedes desactivar el micrófono cuando no lo uses (tiene un botón con un icono de micrófono tachado).
2. Abre la App > “Más” > “Configuración” > “Privacidad de Alexa”.
3. Allí puedes borrar las grabaciones de voz.

• Borra y revisa tu historial de voz en Alexa

1. Abre la aplicación Alexa en tu móvil.
2. Entra en Más > Configuración > Privacidad de Alexa.
3. Localiza la opción “Revisar historial de voz” y elimina las grabaciones.
4. Activa la opción para que Alexa no guarde las grabaciones automáticamente.



ÍNDICE

• Compra con seguridad

Alexa puede hacer compras mediante voz. Si no lo necesitas, desactiva esta opción:

1. App > “Más” > “Configuración” > “Configuración de cuenta” > “Compras por voz”.
2. Puedes desactivarlas o pedir un PIN de seguridad antes de confirmar una compra.

Control parental

Si hay menores en casa, activa las restricciones de Alexa para limitar el acceso a los contenidos de pago y realización de compras usando la voz.

3. Usa Alexa de manera responsable

1. Coloca Alexa en un lugar donde no se escuchen conversaciones privadas (por ejemplo, mejor en el salón que en el dormitorio).
2. No le dictes información personal sensible (número de cuenta, contraseñas, DNI).
3. Mantén el dispositivo y la App siempre actualizados para evitar fallos de seguridad.

↑
ÍNDICE



8.3

Configura las notificaciones de aplicaciones y juegos para evitar publicidad engañosa, estafas y cobros no deseados

1. ¿Por qué es importante controlar las notificaciones?

- Evitas distracciones constantes.
- Reduces la posibilidad de caer en publicidad engañosa o enlaces peligrosos.
- Solo recibes lo que realmente es útil para ti: mensajes, recordatorios, citas médicas.

2. Cómo hacerlo en Android

1. Abre los Ajustes de tu móvil.
2. Pulsa en Notificaciones.
3. Verás una lista de todas las aplicaciones instaladas.
4. Busca la aplicación o juego que envía publicidad.
5. Pulsa sobre ella y selecciona:

- Bloquear notificaciones (si no te interesa recibir nada).
- O bien desactivar solo “Notificaciones promocionales” y dejar activadas las importantes.

3. Cómo hacerlo en iPhone (iOS)

1. Abre los Ajustes.
2. Pulsa en Notificaciones.
3. Selecciona la aplicación que quieras configurar.
4. Desactiva la opción Permitir notificaciones, o bien ajusta:
 - “En pantalla bloqueada”.
 - “En el centro de notificaciones”.
 - “Banners”.



ÍNDICE

4. Consejos extra de seguridad

- Desconfía de anuncios que prometen premios, dinero o regalos

- No pulses enlaces que aparecen en notificaciones sospechosas

- Si una App envía demasiada publicidad, considera desinstalarla

- Descarga aplicaciones sólo desde Google Play o App Store

- Antes de instalar una App, lee los comentarios y valoración de las personas que la usaron

- Comprueba que la App no utilice cargos adicionales y desactívalos cuando te sea posible



↑
ÍNDICE

9. Mantenimiento y respaldo de información

Nuestros dispositivos digitales almacenan información valiosa y perderla es un problema. Este apartado te mostrará cómo mantener tus dispositivos y hacer copias de seguridad para proteger tus recuerdos y documentos, asegurando que siempre puedas recuperarlos y manteniendo tu tranquilidad digital.

9.1

Copia de seguridad

1. ¿Qué es y por qué es importante?

↑
ÍNDICE

Una copia de seguridad es una copia de tus archivos importantes (fotos, contactos, documentos, vídeos, etc.) que se guarda en otro lugar, por si se pierde, borra o estropea el dispositivo.

Hacer una copia de seguridad de forma periódica es importante porque:

- Protege tus recuerdos (fotos y vídeos) y documentos importantes.
- En caso de virus o robo, puedes recuperar todo fácilmente.
- Si cambias de móvil, no pierdes tus contactos ni archivos.
- Te da tranquilidad.

2. ¿Cómo hago una Copia de Seguridad?

En móviles Android (Samsung, Xiaomi, Motorola...)

1. Abre “Ajustes”.
2. Ve a “Cuentas y copia de seguridad” o “Sistema > Copia de seguridad”.
3. Activa “Copia en Google Drive”.
4. Asegúrate de que incluya fotos, contactos, aplicaciones, y mensajes.
5. Google ofrece hasta 15 GB gratis en la nube.

En iPhone

1. Abre “Ajustes”.
 2. Pulsa en tu nombre (arriba) > “iCloud”.
 3. Entra en “Copia en iCloud”.
 4. Activa la opción.
- Apple ofrece 5 GB gratis (puedes ampliar espacio si lo necesitas).

En un ordenador con un disco duro externo o USB:

1. Conecta el dispositivo al ordenador.
2. Abre la carpeta donde tengas tus archivos.
3. Copia (Ctrl + C) y pega (Ctrl + V) en el disco externo.
4. Guarda documentos, fotos, vídeos, música, etc.

En un ordenador usando servicios en la nube (como Google Drive o OneDrive):

1. Entra en <https://drive.google.com> (Google) o <https://onedrive.live.com> (Microsoft).
2. Inicia sesión con tu cuenta.
3. Pulsa en “Subir archivo” o “Subir carpeta”.
4. Elige lo que quieras guardar.

TIPOS DE COPIAS DE SEGURIDAD

Tipo	¿Dónde se guarda?	Ventajas
En la nube	En Internet (Google Drive, iCloud...)	Automáticas, accesibles desde cualquier lugar
Disco duro externo	Dispositivo físico conectado al ordenador	Gran capacidad, no depende de Internet
Memoria USB	Pequeño y fácil de usar	Ideal para documentos y fotos

3. ¿Cuándo hago una Copia de Seguridad?



ÍNDICE

- Una vez al mes es un buen hábito.
- Si haces muchos cambios o tomas muchas fotos, puedes hacerla una vez por semana.
- Siempre haz una copia antes de cambiar de móvil o formatear el equipo.



9.2

Limpieza de archivos obsoletos y del caché

El mantenimiento del móvil es uno de los problemas más comunes. Así que, para no tener problemas de espacio, es importante gestionar muy bien el almacenamiento. Ya que no nos dejará instalar más aplicaciones y muchas de las aplicaciones instaladas dejarán de funcionar correctamente al desactivarse su sincronización. Esto puede ocasionar que dejemos de recibir mensajes, notificaciones y otros avisos hasta que hagamos una limpieza para liberar espacio.

Para que nuestro dispositivo funcione de forma adecuada tenemos que hacer limpieza del almacenamiento. Éstas son sólo algunas recomendaciones para poder liberar espacio.

1. ¿Por qué es importante borrar archivos obsoletos y la caché?

Cuando usamos el teléfono, se van acumulando datos que ya no necesitamos, como:

- Archivos temporales (caché).
- Fotos duplicadas o descargadas de WhatsApp.
- Archivos antiguos que ocupan espacio.

Si no se limpian de vez en cuando, pueden provocar:

- Menos espacio disponible.
- El teléfono funciona más lento.
- Más riesgo de fallos y errores.

2. ¿Qué es la Caché?

La caché son datos que las aplicaciones guardan para abrir más rápido. Por ejemplo, imágenes de una página web o datos de una aplicación. Con el tiempo, estos datos pueden ocupar mucho espacio y ralentizar tu dispositivo.



ÍNDICE

¿Cómo borrar archivos obsoletos y la caché en Android?

Opción 1: Usando “ajustes”

1. Abre Ajustes (icono de engranaje ).
 2. Pulsa “Almacenamiento”.
 3. Verás cuánto ocupan aplicaciones, imágenes, etc.
 4. Pulsa en “Datos en caché” y confirma que quieres borrar la caché.
- Esto no borra tus fotos ni tus datos personales.

Opción 2: Borrar la caché de una sola App

1. Ajustes > Aplicaciones.
2. Elige la App que quieres limpiar (por ejemplo, WhatsApp).
3. Pulsa en “Almacenamiento”.
4. Pulsa “Borrar caché”.

Opción 3: Usar un “Limpia Móvil”

Muchos móviles tienen una App llamada “Mantenimiento del dispositivo” o “Administrador de archivos” que ayuda a eliminar archivos basura.

1. Abre esa App.
2. Pulsa “Limpiar” u “Optimizar”.

↑
ÍNDICE



¿Cómo borrar archivos obsoletos y la caché en iPhone?

En iPhone no existe un botón para borrar toda la caché de una vez, pero puedes hacerlo de esta manera:

- Borrar caché del navegador (Safari):

1. Abre Ajustes.
2. Baja hasta Safari.
3. Pulsa “Borrar historial y datos de sitios web”.

- Limpiar caché de aplicaciones:

Si una App ocupa demasiado espacio:

1. En Ajustes > General > Almacenamiento del iPhone.
2. Verás la lista de Apps y cuánto ocupan.
3. Si quieres liberar espacio:

- Pulsa en la App.

- Puedes Eliminar App y volver a instalarla (esto limpia su caché).

- Eliminar fotos y archivos que ya no uses:

1. Abre la App Fotos.
2. Elimina capturas antiguas o imágenes repetidas.
3. Vacía la carpeta “Eliminado recientemente” para liberar espacio.

¿Qué beneficios tiene?

- El móvil funciona más rápido.
- Recuperas espacio para fotos y Apps nuevas.
- Evitas errores y problemas de funcionamiento.

Consejos prácticos

- Haz esta limpieza una vez al mes.
- Antes de borrar, revisa que no eliminas documentos importantes.
- Si no estás seguro, pide ayuda a un familiar o persona de confianza.

↑
ÍNDICE

10. Recursos y redes de apoyo

Si quieres aprender más sobre tecnología, resolver dudas o pedir ayuda si algo sale mal, no estás solo/a.

10.1 Teléfonos y páginas de ayuda oficial

INCIBE



017 Teléfono gratuito de ayuda en ciberseguridad (para toda España).



Horario: Todos los días de 9:00 a 21:00 h.



www.incibe.es

Te ayudan si:

- Sospechas que te han estafado.
- Te han robado datos.
- Necesitas consejo sobre seguridad digital.



ÍNDICE

Oficina de Seguridad del Internauta (OSI)

Información práctica y alertas de seguridad.



www.osi.es

Policía Nacional y Guardia Civil

Para denunciar delitos informáticos:

- Policía Nacional: 091
- Guardia Civil: 062
- También puedes acudir a tu comisaría o cuartel más cercano.

Plan Nacional de Competencias Digitales

Iniciativa estatal para acercar la tecnología a toda la ciudadanía.



www.inclusion.gob.es/digitalizacion

Junta de Andalucía – Puntos Vuela

Más de 750 centros públicos con talleres de informática y apoyo.



www.andaluciavuela.es/personas/puntos-vuela/

10.2

Canales y servicios para la inclusión digital de personas mayores

Junta de Andalucía – Juntate



900 100 300 Teléfono gratuito de ayuda y atención personalizada para personas mayores de Andalucía en situación de soledad no deseada.



Horario: Todos los días de 8:00 a 20:00 h.



www.juntate.es

En esta página de la Junta de Andalucía encontrarás apoyo, recursos e información para afrontar la soledad no deseada. Aquí descubrirás actividades, consejos y servicios diseñados especialmente para las personas mayores.

Juntate

Si te sientes en soledad, Andalucía te acompaña



ÍNDICE

Centros de Participación Activa de Personas Mayores

Los Centros de Participación Activa son centros de promoción del bienestar de las personas mayores tendentes al fomento de la convivencia, la integración, la participación, la solidaridad y la relación con el medio social. Puedes consultar tu Centros de Participación Activa de Personas Mayores más cercano en el siguiente enlace:



11. Glosario de términos sobre Seguridad Digital

A continuación, veremos varios escenarios y elementos básicos que son clave dentro del mundo de la ciberseguridad:

- **Actualización:** Mejora que se instala en un dispositivo o aplicación para corregir errores, aumentar la seguridad o mejorar su funcionamiento.
- **Antivirus:** Programa que detecta y elimina virus o amenazas en el móvil, ordenador o tableta. Es importante mantenerlo actualizado.
- **App (Aplicación):** Programa que se instala en el móvil o tableta y sirve para realizar tareas como enviar mensajes, hacer videollamadas o consultar el banco.
- **Archivo adjunto:** Documento o imagen que acompaña a un correo electrónico. No se debe abrir si el remitente es desconocido.
- **Banca online:** Servicio que permite hacer operaciones bancarias desde Internet: consultar el saldo, pagar recibos o hacer transferencias.
- **Barra de direcciones:** Espacio en la parte superior del navegador donde se escribe la dirección web (URL) de la página que se quiere visitar.
- **Biometría:** Método para desbloquear el dispositivo usando partes del cuerpo, como la huella dactilar o el rostro.
- **Bluetooth:** Conexión inalámbrica para compartir archivos o conectar dispositivos entre sí, como un móvil y unos auriculares.
- **Bulos:** Mensajes falsos que se comparten para confundir o alarmar. Suelen llegar por redes sociales o WhatsApp.
- **Buscador:** Herramienta como Google que sirve para buscar información en Internet.
- **Caché:** Memoria temporal que guarda datos de páginas visitadas para que se carguen más rápido. Se puede borrar para liberar espacio.
- **Certificado digital:** Archivo electrónico o icono (candado) que indica que una web es segura. También puede ser un sistema de identificación para hacer trámites oficiales online.



ÍNDICE

- **Ciberacoso:** Acoso a través de medios digitales, como mensajes ofensivos o amenazas por redes sociales o correo electrónico.
- **Cifrado:** Proceso que protege la información haciendo que solo pueda ser leída por quien tenga la clave.
- **Conexión Wi-Fi:** Sistema que permite conectarse a Internet sin usar cables. Es importante que esté protegida con contraseña.
- **Contraseña (*Password*):** Clave secreta para acceder a cuentas o dispositivos. Debe ser segura (larga, con números y símbolos).
- **Cookies:** Pequeños archivos que guardan información de la navegación en una página web, como idioma, preferencias o hábitos de uso.
- **Copia de seguridad:** Copia de archivos importantes (fotos, contactos, etc.) que se guarda en otro lugar (nube, USB, disco externo) para no perderlos.
- **Cortafuegos (Firewall):** Sistema que bloquea accesos no autorizados a un dispositivo conectado a Internet.
- **Correo electrónico:** Servicio para enviar y recibir mensajes a través de Internet.
- **Datos personales:** Información como nombre, DNI, teléfono o cuenta bancaria. No deben compartirse sin precaución.
- **Descarga segura:** Acción de bajar aplicaciones o archivos desde sitios oficiales para evitar virus o fraudes.
- **Dispositivo:** Aparato digital como el móvil, ordenador, tableta o reloj inteligente que se usa para conectarse y realizar tareas.
- **Enlace (Link):** Texto o imagen que, al hacer clic, lleva a otra página o contenido en Internet.
- **Estafa digital (fraude online):** Engaño que se realiza a través de medios digitales para obtener dinero o datos personales.
- **Fake news (Noticias falsas):** Noticias que parecen reales pero son mentira. Se difunden para engañar o manipular.
- **Historial:** Lista de páginas web visitadas guardada en el navegador.
- **HTTP / HTTPS:** Protocolos de navegación. Si la página comienza por “https”, es más segura y sus datos están cifrados.
- **Identidad digital:** Conjunto de datos, imágenes y acciones que nos representan en Internet.
- **Malware:** Programa malicioso (virus, troyano, espía...) diseñado para dañar un dispositivo o robar información.
- **Navegador web:** Programa que permite visitar páginas de Internet (como Chrome, Firefox, Safari o Edge).

- **NFC:** Tecnología para pagar con el móvil sin contacto, igual que las tarjetas “contactless”.
- **Nube (Almacenamiento en la nube):** Espacio en Internet para guardar archivos y poder acceder desde cualquier dispositivo.
- **Online:** Se refiere a estar conectado a una red de datos (Internet) o a algo que está disponible a través de Internet.
- **Permisos (de Apps):** Accesos que una aplicación solicita para funcionar (por ejemplo, a la cámara, ubicación o contactos).
- **Phishing:** Estafa en la que se hacen pasar por una entidad conocida (como un banco) para robarte datos.
- **Pop-ups:** Ventanas emergentes que aparecen al navegar. A veces son publicidad o enlaces maliciosos.
- **Redes sociales:** Plataformas como Facebook, Instagram o WhatsApp donde se puede compartir fotos, mensajes y mantenerse en contacto.
- **Router:** Aparato que permite la conexión a Internet en casa.
- **Smishing:** Estafa que llega por mensaje SMS, donde intentan engañarte para robar tus datos.
- **Software:** Programa que se instala en el dispositivo para realizar una tarea específica (correo, juegos, navegador...).
- **Software pirata:** Programa descargado de fuentes no oficiales. Puede contener virus o ser ilegal.
- **Spam:** Correo no deseado, generalmente publicitario. Puede ser molesto o contener estafas.
- **Suplantación de identidad:** Cuando alguien se hace pasar por ti en Internet sin tu permiso.
- **URL:** Dirección web que permite acceder a una página en Internet. Suele comenzar por “https://”.
- **Verificación en dos pasos:** Medida de seguridad que añade un código extra (enviado al móvil) al iniciar sesión, además de la contraseña.
- **Videollamada:** Llamada que permite verse y hablar con otra persona usando el móvil o el ordenador con cámara.
- **Virus informático:** Programa dañino que afecta al funcionamiento de un dispositivo o roba información.
- **Vishing:** Estafa mediante llamada telefónica, donde el estafador finge ser alguien de confianza para obtener datos o acceso.



Junta de Andalucía