Fundación Telefónica

GUÍA DEL ALUMNO

Ciberseguridad básica

Nombre:

Gracias por acudir a nuestro taller de formación. Esperamos que te haya sido útil, además de pasar un buen rato.

Con esta breve guía **queremos que tengas en casa temas explicados, cosas aprendidas** y alguna más que quizá se haya quedado en el tintero.

A lo largo de las páginas encontrarás un resumen de los siguientes bloques temáticos, que te resultarán ya familiares:

1. **Qué es la ciberseguridad**
2. **Gestión de contraseñas**
3. **Protección de dispositivos**
4. **Navegación segura**
5. **Identificar las estafas**

Esta guía pretende proporcionarte algunas indicaciones para tener en cuenta a la hora de desarrollar la formación en cada uno de los bloques.

Esperamos que te sirva de apoyo.

Fundación Telefónica

1

QUÉ ES LA CIBERSEGURIDAD

1. Qué es la ciberseguridad

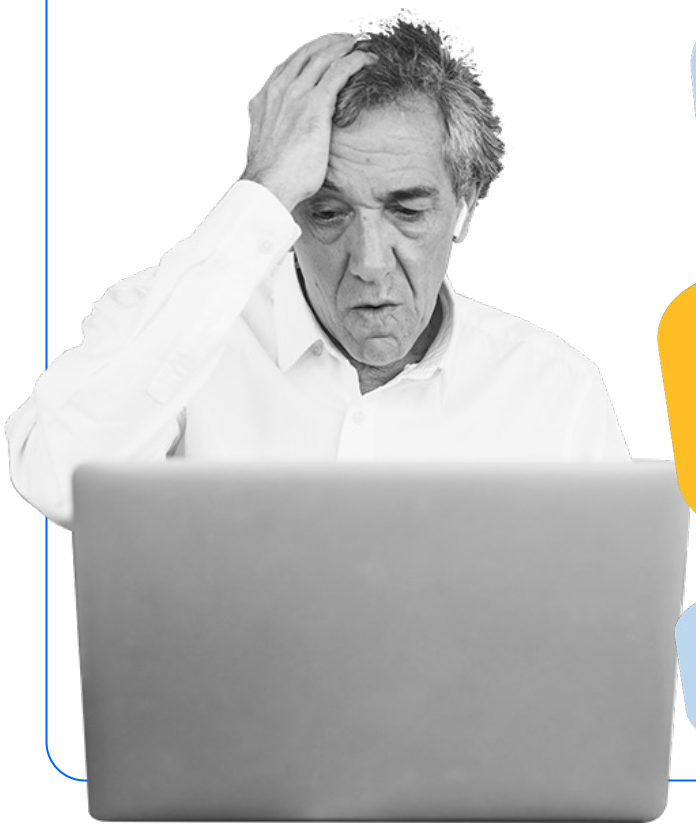
Introducción

Objetivos

- Gestionar adecuadamente nuestros dispositivos y aplicaciones con el fin de estar protegidos.
- Conocer algunas herramientas para navegar de forma más segura y privada.
- Detectar y gestionar posibles riesgos.

¿Qué es la ciberseguridad?

- La **ciberseguridad** es el conjunto de prácticas que llevamos a cabo para **proteger nuestros dispositivos** de posibles riesgos mientras navegamos por internet.
- Y, ¿qué es un **ciberataque**? Es una acción intencionada llevada a cabo con objeto de **robar, exponer o destruir datos** a través de un acceso no autorizado a nuestros dispositivos.



Que tu dispositivo esté en reposo **no elimina ningún riesgo**, ya que sigue estando conectado a internet

¿**Cómo sabes** si tu dispositivo **está en reposo**? Si se enciende al pulsar ligeramente un botón lateral o sobre la pantalla.

El móvil está en *standby* siempre que no lo apaguemos totalmente.

1. Qué es la ciberseguridad

Reflexiona

¿Crees que la ciberseguridad o los ciberataques nos afectan a todos nosotros?
¿O es, por el contrario, un tema que influye más a las grandes empresas?

¿Por qué debemos **proteger** nuestros dispositivos y **navegar** con seguridad?

- En nuestro teléfono almacenamos mucha **información personal**: mensajes, direcciones, fotografías...
- A través de internet enviamos y recibimos **muchos datos**: contraseñas, documentos, dinero...

Fundación Telefónica

2

GESTIÓN DE CONTRASEÑAS

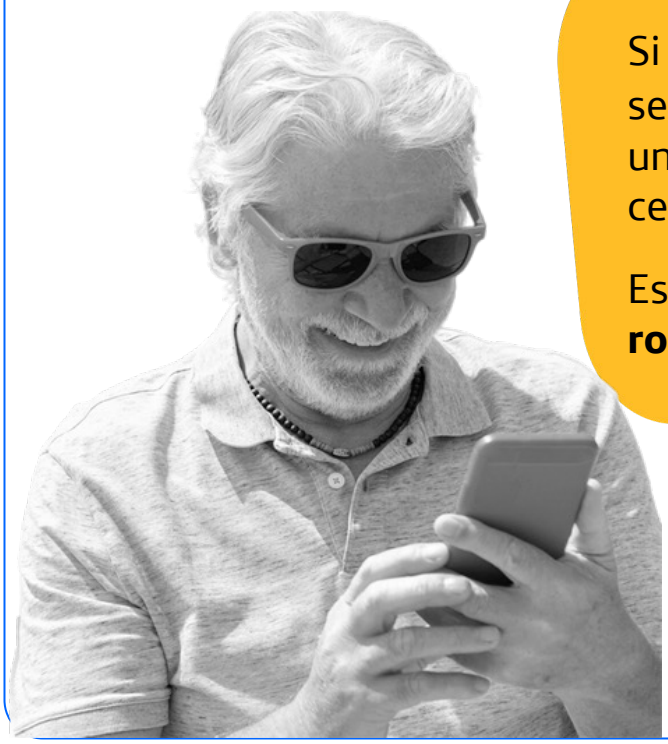
2. Gestión de contraseñas

La contraseña es uno de los primeros **mecanismos de defensa** que tienes para ayudar a proteger tus datos.

Una contraseña o password es una **serie secreta** de letras, números y signos que protegen el acceso a un servicio de internet, a una aplicación o a tu teléfono.

¿Cierras la **puerta** de tu casa con **llave** cuando te vas?

En el teléfono, esa llave sería tu **contraseña**.



Si la puerta es blindada y la llave de seguridad, serán más seguras que una puerta antigua con una cerradura sencilla.

Es recomendable usar **contraseñas robustas**.

Características de una contraseña segura

****

- ¿Usarías **la misma llave** para tu casa, tu coche, tus maletas?...
- Al igual que con las llaves, debe utilizarse una **contraseña distinta** para cada cosa. Si usas la misma para todo y alguien la roba, el ladrón tendrá acceso a todas tus cosas.
- Una contraseña debe ser relativamente **simple**, para poder recordarla, pero a la vez **segura**.

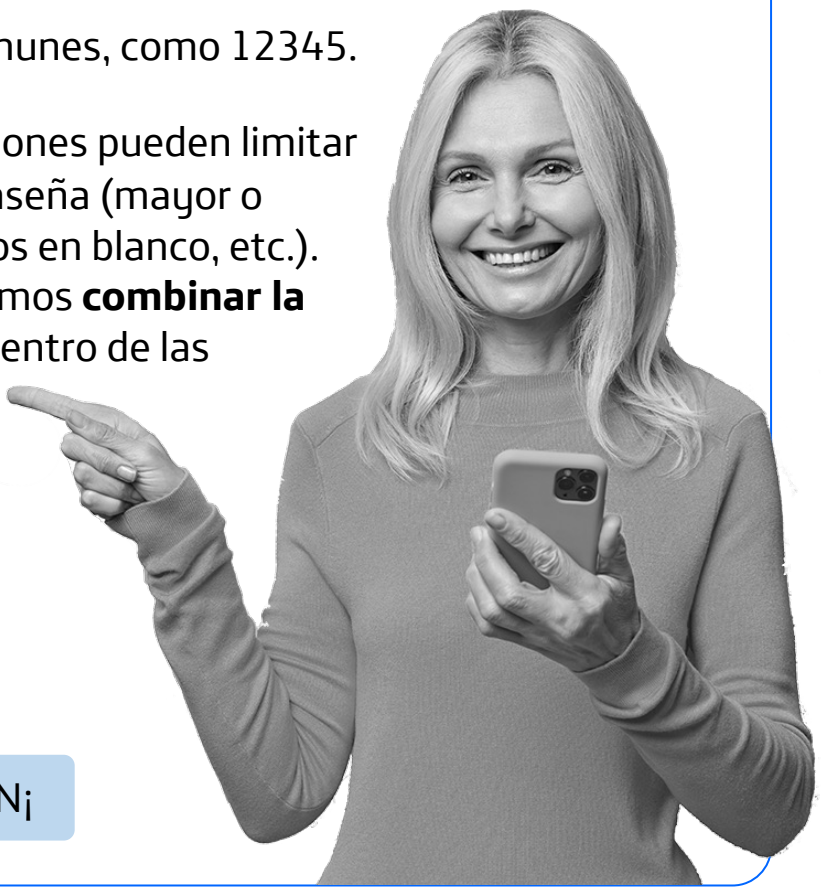
Evita fechas de nacimiento y otros detalles personales.

Evita contraseñas comunes, como 12345.

Algunos servicios o aplicaciones pueden limitar la composición de la contraseña (mayor o menor longitud, sin espacios en blanco, etc.). En ese caso, te recomendamos **combinar la mayor variedad posible** dentro de las posibilidades permitidas:

- Minúsculas.
- Mayúsculas.
- Números.
- Símbolos.

Por ejemplo: 4yU_*so7)@N¡



2. Gestión de contraseñas

En la actualidad, se recomienda utilizar un conjunto de palabras (***passphrase***) con al menos **16 caracteres**. Puedes utilizar una frase de un libro o una película, por ejemplo:

anoche soñé que volvía a manderley

No utilices datos personales o demasiado tópicos. Si todo el mundo sabe que eres fan de Hitchcock, cambia de frase.

houston tenemos un problema

Si es posible, utiliza mayúsculas y signos de puntuación, y añade alguna variación con números o símbolos.

¡Houston, tenemos 2 problemas!

- Si tienes muchas contraseñas, será imposible recordarlas todas sin ayuda. En ese caso, puedes acudir a un **gestor de contraseñas**, que es una aplicación que sirve para almacenarlas en un formato seguro, imposible de descifrar.
- Algunos gestores son **gratuitos** (ej: KeePass) y otros gratuitos, pero con **versión de pago** para acceder a todas sus funciones (ej: EnPass, 1Password, Bitwarden).

3

PROTECCIÓN DEL DISPOSITIVO

3. Protección del dispositivo

En tu teléfono, aun sin darte cuenta, guardas mucha **información delicada** y **confidencial**: contactos, fotografías, mensajes, información de aplicaciones financieras o de salud, etc.

Esta información podría dejar al descubierto a las personas con las que te relacionas, tus hábitos y planes de futuro.

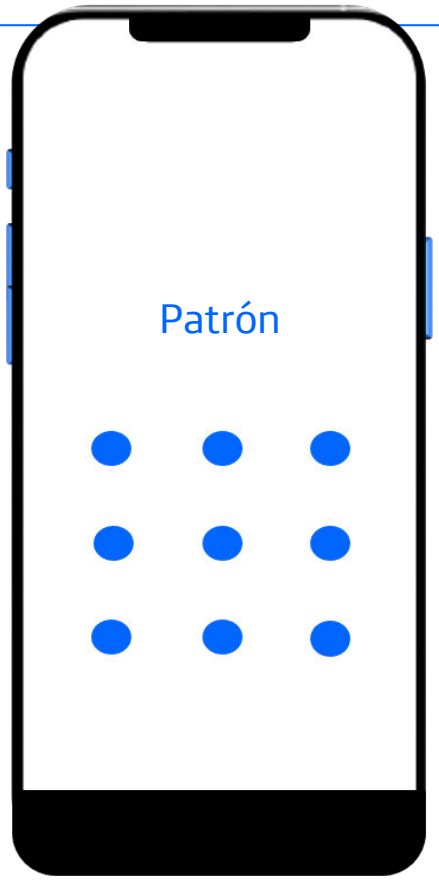
3.1. Bloqueo de pantalla

¿Recuerdas que las contraseñas son como las llaves para entrar a tu casa? Del mismo modo, el **bloqueo de pantalla** es la manera de **proteger el acceso** a tu teléfono.

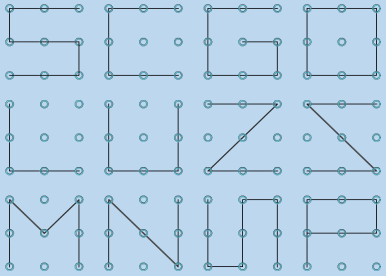
El bloqueo de pantalla puede llevarse a cabo de **distintas maneras**.

Pulsa en el icono de ajustes y sigue estos pasos:

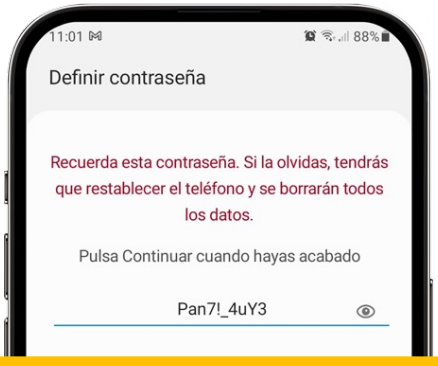
3. Protección del dispositivo

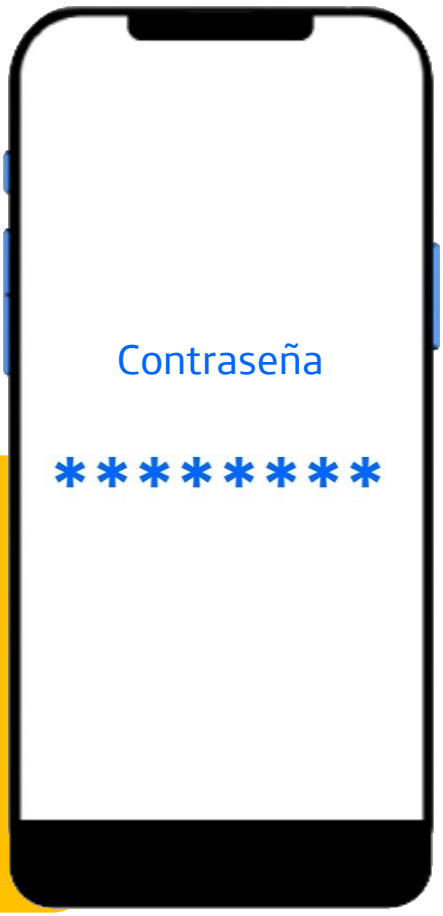


- Sistema de trazado de dibujo con el dedo uniendo una serie de nueve puntos.
- A la hora de crear un patrón debes intentar evitar algunos de los más comunes, como la **M**, la **L** y o la **Z**, en ambas direcciones.



- Usar 8 puntos de manera aleatoria permite crear un patrón seguro.





La contraseña puede incluir letras y números, así que será mucho más segura que un PIN normal de 4 o 6 dígitos, siempre y cuando tenga esa longitud, aunque también más pesado de teclear.

Puede resultar más fácil utilizar un **PIN largo** que una contraseña más corta, obteniendo el **mismo nivel** de seguridad.

3. Protección del dispositivo

Hay que introducir un código numérico entre 4 y 16 dígitos.

Cuantos más dígitos, más seguro será el código.

Algunos teléfonos pueden leer las huellas dactilares y utilizarlas como contraseña.

Similar al bloqueo con huella dactilar, pero reconociendo los rasgos faciales.

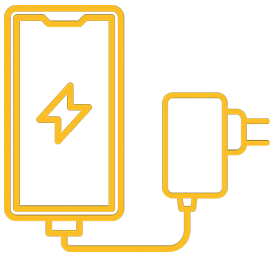
3.2. Actualizaciones

Las **actualizaciones** del teléfono y las aplicaciones sirven para mejorar sus **funcionalidades** y la **seguridad** del dispositivo.

- Elige las actualizaciones automáticas si es posible.
- Instala las actualizaciones cuanto antes.
- Actualiza siempre las aplicaciones desde la tienda oficial: Play Store (Android) o App Store (iOS).

Actualización del sistema

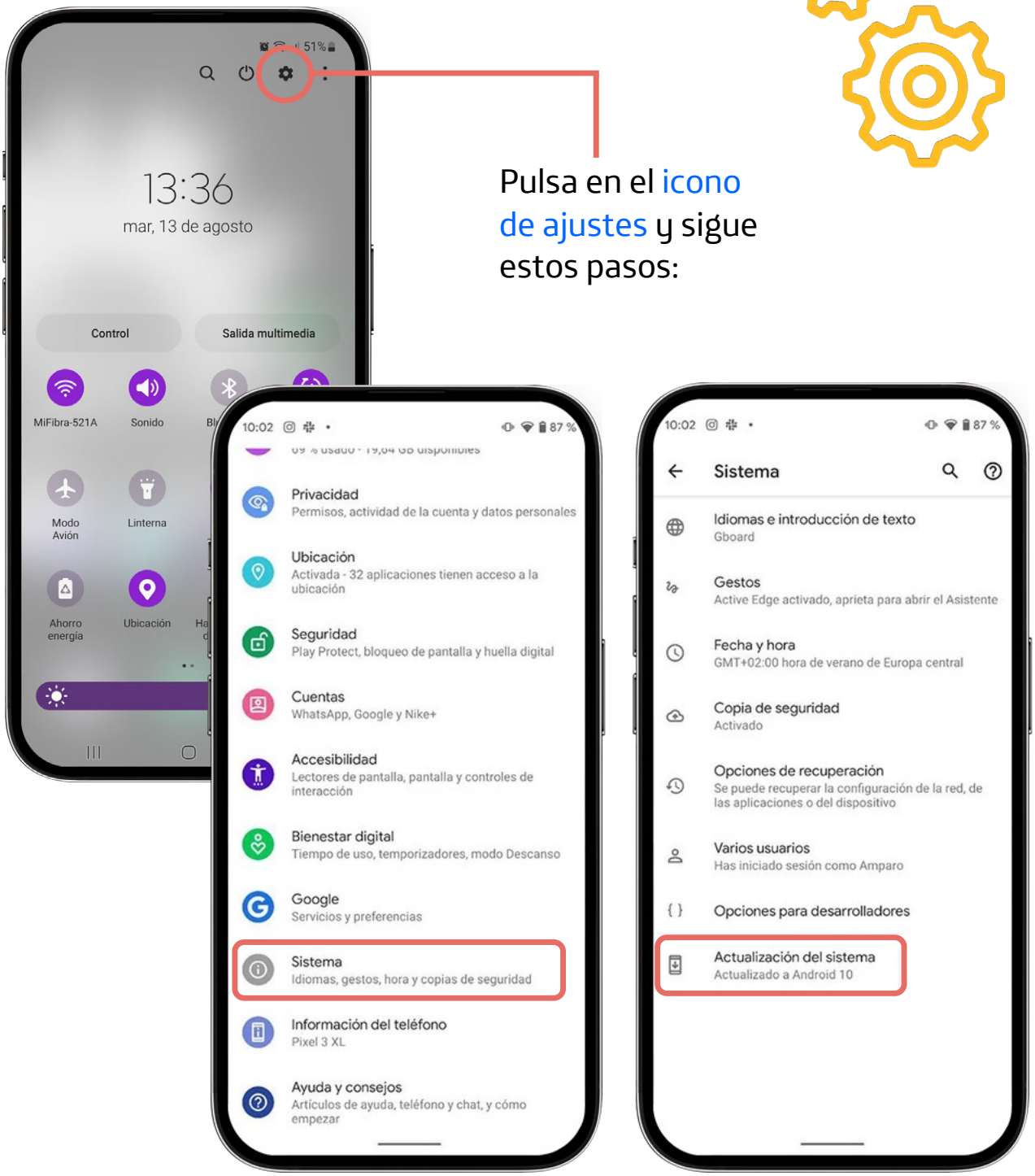
Para actualizar el sistema operativo debes estar conectado a una red **Wi-Fi** y tener el **teléfono enchufado** al cargador, por si la actualización se demora y te quedas sin batería.



La ubicación de la actualización del sistema operativo puede variar según el fabricante. Las localizaciones más habituales:

- Ajustes → Actualización de software (o del sistema)
- Ajustes → Sistema → Actualización de software
- Ajustes → Sistema → Ajustes avanzados → Actualización de software
- Ajustes → Información del teléfono (o Sobre el teléfono) → Actualizaciones del sistema
- Ajustes → General → Acerca del teléfono → Actualizar SW

Actualización del sistema

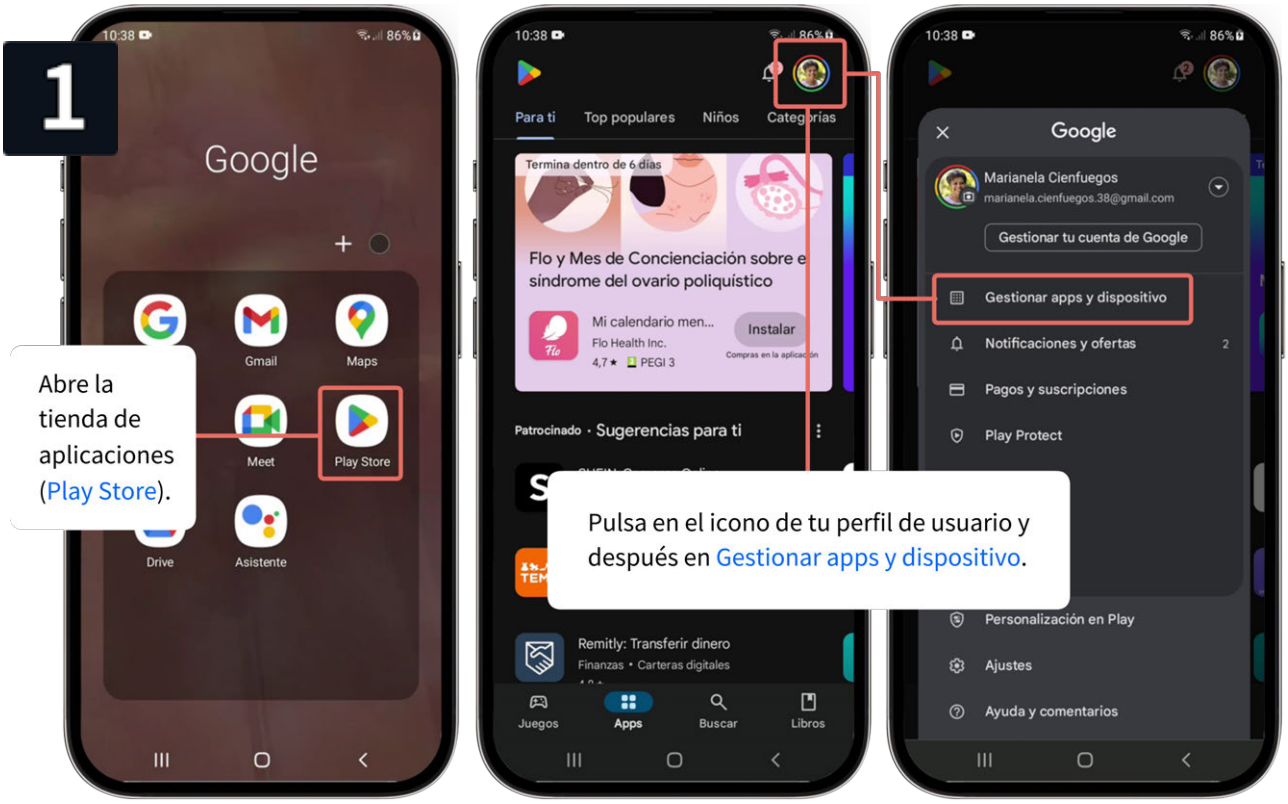


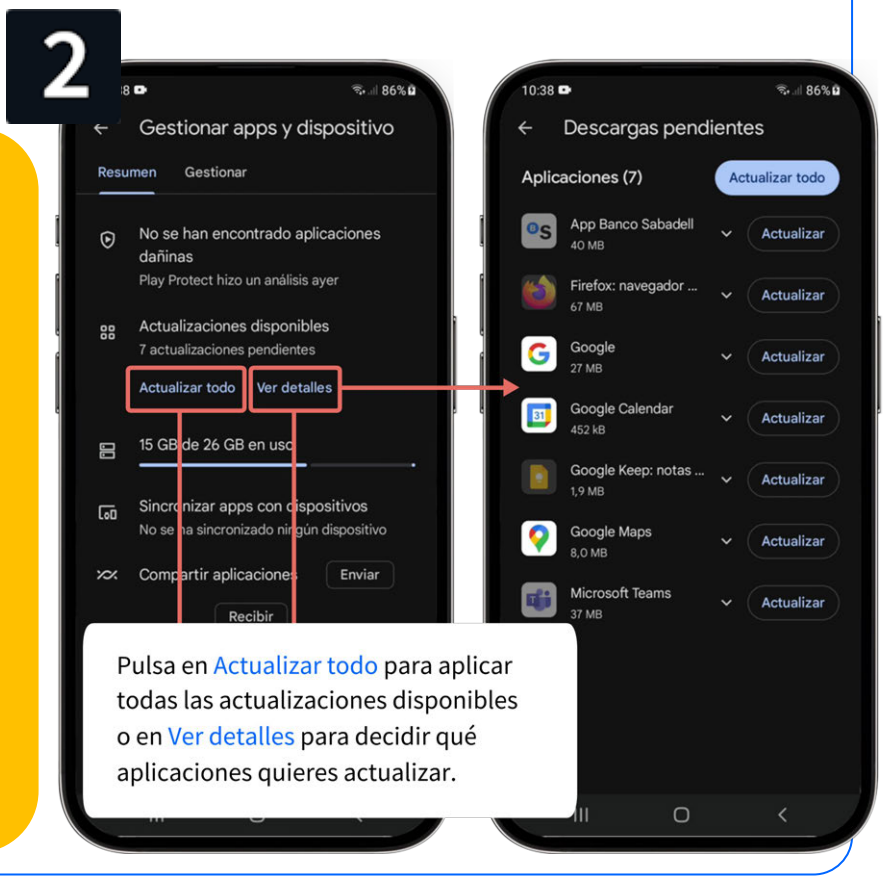
Pulsa en el icono de ajustes y sigue estos pasos:

3. Protección del dispositivo

Fundación Telefónica

Actualización de las aplicaciones



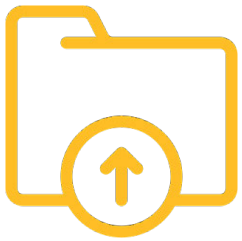


Las aplicaciones son programas que se instalan en el teléfono y te permiten **realizar tareas**.
Algunas ya vienen instaladas en el teléfono: el calendario para apuntar las citas, los contactos o la aplicación para llamar por teléfono.
Otras puedes instalarlas tú desde la tienda de aplicaciones: WhatsApp para comunicarse, Cita Sanitaria para los médicos, Google Maps para planificar rutas...

Copia de seguridad

Una copia de seguridad es un **duplicado de tus datos** en un lugar seguro de internet. Puedes utilizar ese duplicado para poner la información en un teléfono nuevo. Esta copia puede hacerse de manera **automática**.

- Conserva los datos de tu teléfono.
- Obtén facilidades para instalar y poner en marcha un nuevo teléfono.
- Sin pérdidas de información.

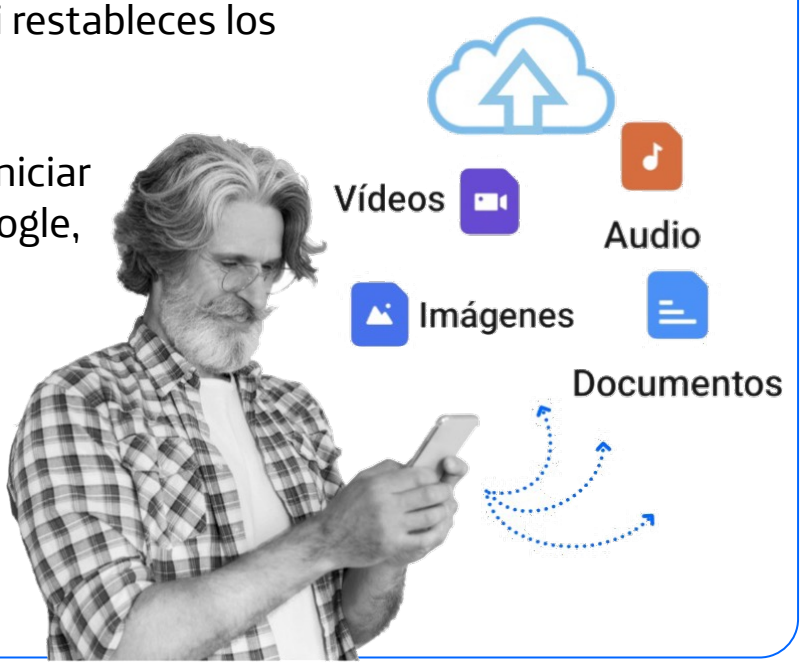


Una vez creada la copia de seguridad, esta permanece **inalterable**. Si borras de tu teléfono contactos o el historial de llamadas, estos seguirán existiendo en la copia de seguridad.

Cuando se hace una nueva copia (automática o manual), esta **reemplaza a la anterior**. Si hubieras borrado tus contactos por error, también se perderían, al reemplazar la copia actual a la anterior.

Puedes utilizar la copia de seguridad para restaurar tus datos en otro teléfono (o en el mismo, si restableces los ajustes de fábrica).

Al encender el teléfono e iniciar sesión en tu cuenta de Google, verás una opción para restablecer o sincronizar tus datos.



¿Qué se necesita?

Para realizar una copia de seguridad se necesita una **cuenta de correo electrónico** activa de **Google** (Gmail), ya que la copia se guardará directamente en Google Drive (espacio de almacenamiento en la nube).

Gmail

Correo electrónico de Google: xxxxx@gmail.com

Google Drive

Plataforma de almacenamiento de datos en la nube.

La copia de seguridad de **fotos y vídeos** se hace a través de Google Fotos y funciona igual. La diferencia es que si eliminas una foto por error, antes de eliminarse para siempre permanecerá durante 30 días en la papelera, tanto en tu dispositivo como en la nube de Google Fotos. Aunque la foto borrada pueda rescatarse durante un mes, la foto desaparecerá de la copia de seguridad la próxima vez que se haga una copia, ya que no se hace copia de los contenidos de la papelera.

Cuando pones en marcha un teléfono móvil inteligente, debes usar o abrir una cuenta nueva de correo electrónico.
Las cuentas de Google (xxxxx@gmail.com) vienen con **15 GB de almacenamiento gratuito**. Si necesitas más espacio, tienen distintos planes de pago en su servicio Google One.

En el caso de **iOS**, aunque la cuenta de correo electrónico sea de Gmail, la copia de seguridad se realiza en iCloud (el espacio en la nube de Apple).

3. Protección del dispositivo

Fundación Telefónica

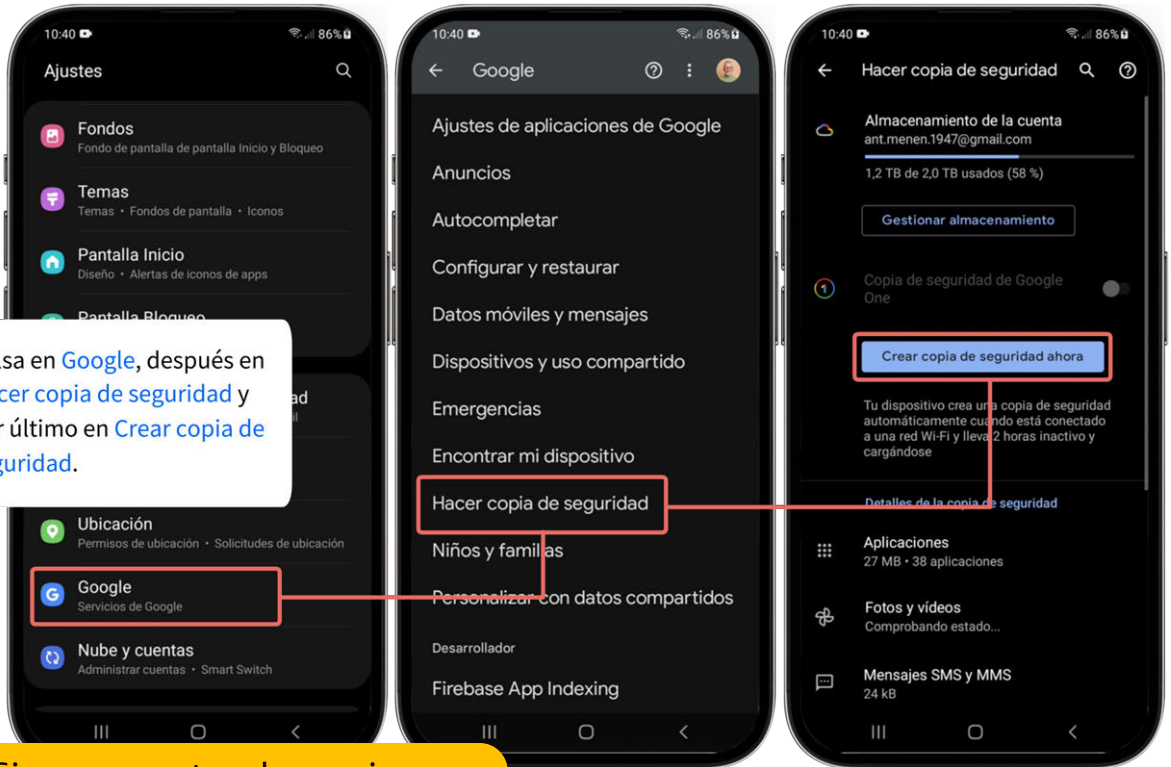
¿Cómo se hace?

1

Desliza desde arriba hacia abajo para mostrar los ajustes rápidos y pulsa en el icono de Ajustes ⚙.

2

Pulsa en Google, después en Hacer copia de seguridad y por último en Crear copia de seguridad.



Si no encuentras las opciones que se muestran aquí, prueba a buscar "copia de seguridad" en tus ajustes o consulta la página web del fabricante.

Si quieres hacer **copia de tus fotos y vídeos**, te pedirá que instales y gestiones tus fotos con Google Fotos

Fundación Telefónica

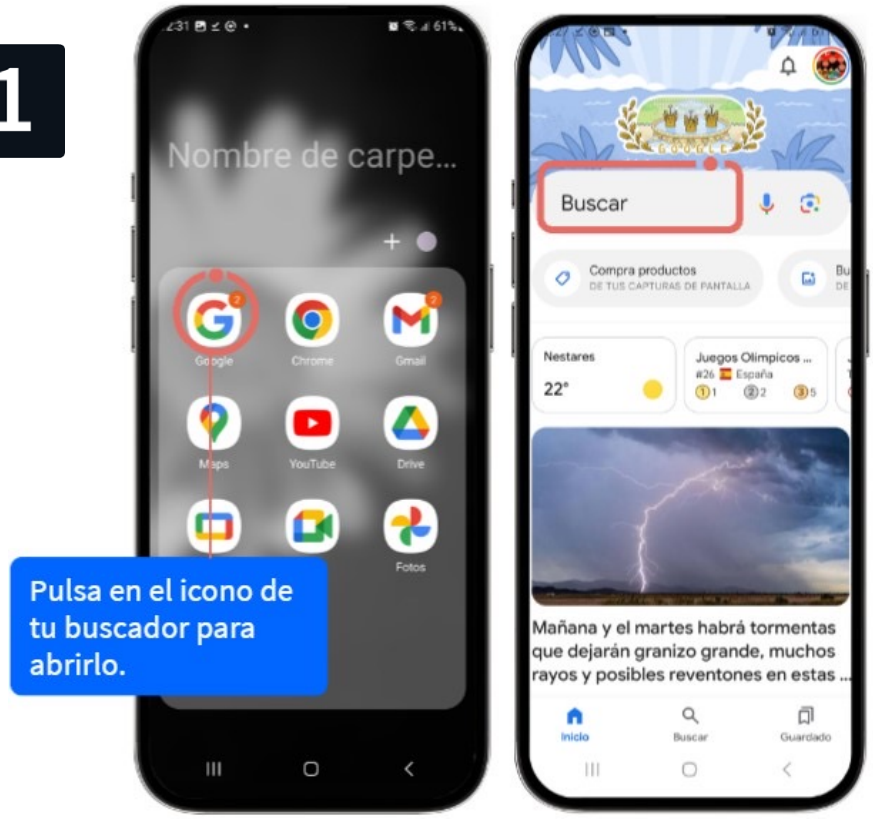
4

NAVEGACIÓN SEGURA

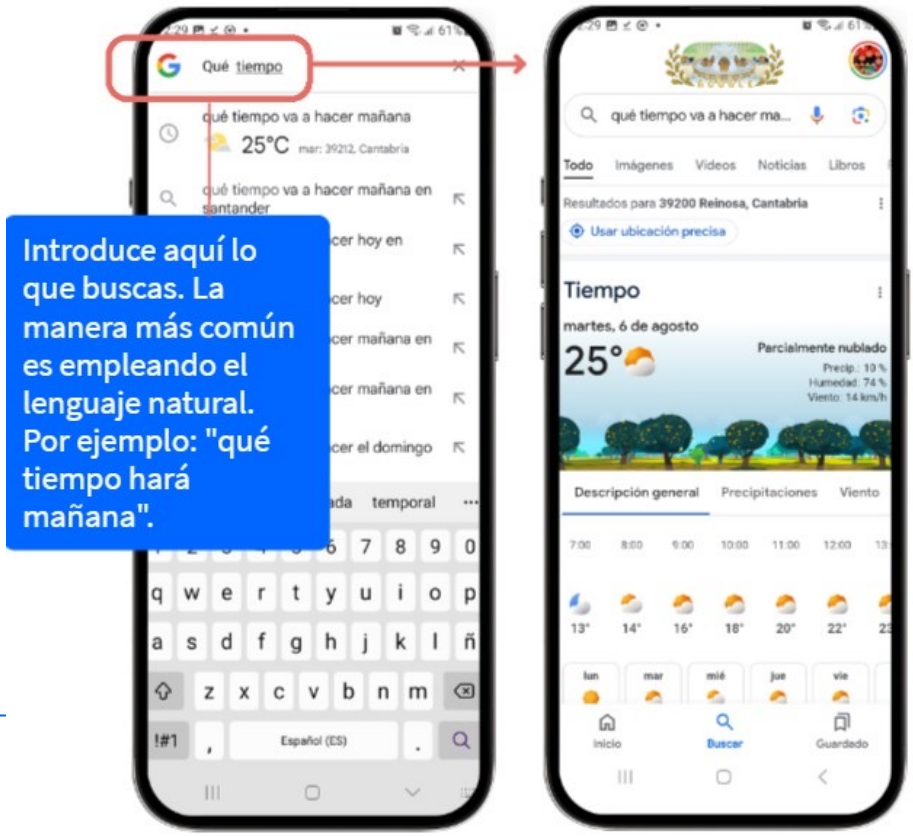
Si te vas de viaje y quieres saber qué tiempo hará en tu destino, ¿qué haces?

Lo buscas en internet.

1



2



4. Navegación segura

- Cada vez que buscas algo, va dejando **rastro** de lo que haces.
- En ocasiones es importante navegar de la manera más **segura** y **privada** posible.

Aunque el uso más común que hacemos de internet es a través de un navegador, hay multitud de aplicaciones y servicios que utilizan internet sin que nos demos cuenta: televisión por cable, correo electrónico, videoconferencias, servicios de música y vídeo, domótica, copias de seguridad y actualizaciones automáticas de nuestros dispositivos, regulación del tráfico, sistemas inteligentes de abastecimiento de agua y luz en las ciudades, telemedicina, videojuegos...

Recuerda que para usar internet necesitas:

Buscador: sistema informático utilizado cuando se está en internet para buscar y encontrar información. Ejemplos: Google, Bing, Yahoo!

Navegador: aplicación que permite acceder a internet, visitar páginas web e interactuar con ellas.Ejemplo: Google Chrome, Safari, Edge o Firefox.

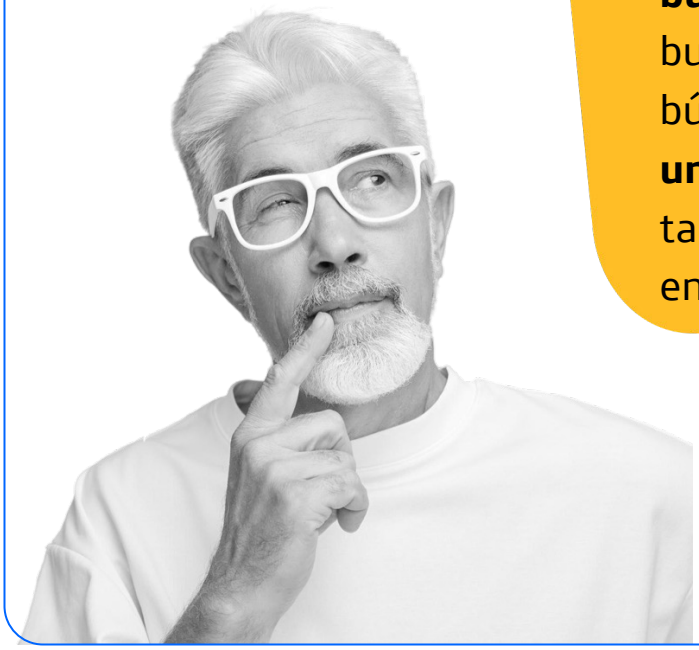
Página web: son los documentos a los que se accede desde el navegador, donde además de texto pueden incluirse imágenes, vídeos y enlaces a otras páginas. Se accede a ellos a través de su dirección o URL. Ejemplo:

https://www.fundaciontelefonica.com/voluntarios/reconectados/

4.1. Navegación privada o "modo incógnito"

La navegación por internet **privada** o en **"modo incógnito"** evita que el navegador guarde **información** sobre las páginas web que has visitado o las búsquedas que hayas realizado.

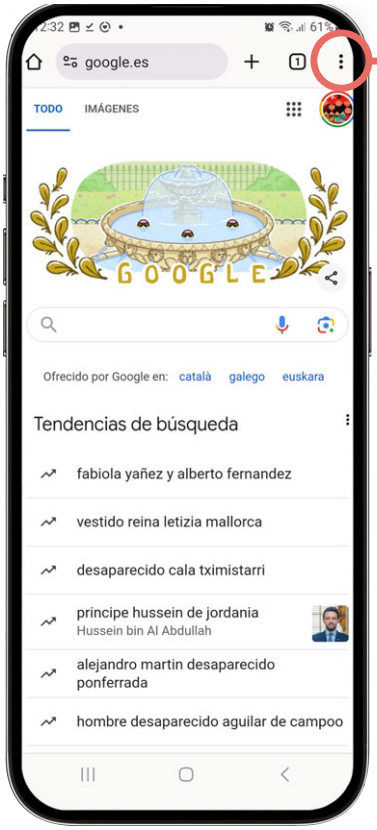
Es recomendable emplear la navegación privada, por ejemplo, si estás utilizando un **ordenador que no es el tuyo** y tienes que rellenar formularios con datos confidenciales, buscar y comprar billetes, etc. De esta manera, el navegador **no almacenará ninguna información** en el dispositivo.



Otro ejemplo: a veces, **cuando buscas billetes** *saben* lo que estás buscando y al realizar la misma búsqueda un rato después, **dan un precio más alto**. En este caso también puede ayudarte navegar en modo incógnito.

4. Navegación segura

Pulsa en el icono de tu **navegador** para abrirlo.



Al pulsar en los tres puntos ⋮ se abrirán distintas **opciones**. Pulsa en Nueva pestaña de incógnito.

- Nueva pestaña
- Nueva pestaña de incógnito
- Historial de navegación
- Favoritos

Una **ventana o pestaña de incógnito** se diferencia de una normal en que el navegador no almacena los sitios que se visitan, no guarda los datos, ni almacena las cookies (lo cual evita, por ejemplo, la publicidad relacionada con las búsquedas, o que una página web "recuerde" que eres su usuario habitual).

¡Atención! Navegar por internet en modo incógnito no hace que tus actividades sean anónimas. Son anónimas únicamente para tu navegador.

Dependiendo del navegador y versión del mismo, el aspecto puede variar o los botones encontrarse en lugares distintos.

4.2. Cookies

¿Te ha sucedido que **al buscar algo en internet** luego ves **publicidad** sobre productos parecidos o relacionados con tu búsqueda?

Esto es debido a las cookies.

Tienen múltiples utilidades:

Las **cookies** son un pequeño fichero de datos que las páginas web que visitas envían a tu navegador.

- **Facilitar la navegación** por las páginas web.
- **Recordar información**: tu identidad, tus preferencias al visitar una web, lo que hay en tu cesta de la compra, etc.
- **Analizar tus actividades y comportamiento**.

Esto último es lo que puede servir para enviarte información relacionada con **tus intereses**.

Las páginas web están obligadas a informarte sobre las cookies que utilizan y pedir tu consentimiento para hacerlo, a causa del **Reglamento General de Protección de Datos**.

Al margen de las cookies que quieran enviar las web, puedes bloquearlas en el navegador buscando en sus Preferencias, en el apartado de Privacidad. Suelen tener una opción para **bloquear las cookies de terceros**, que son las que se usan habitualmente en el ámbito comercial para rastrear nuestras actividades.

Aunque puedas bloquearlas cookies desde el navegador, conviene revisar las políticas de cookies de los sitios web, ya que existen **técnicas de rastreo** diferentes de las cookies. Algunos navegadores incluyen preferencias en el apartado de Privacidad para protegerse de algunas de esas técnicas.

4. Navegación segura

Al abrir las páginas web por primera vez suele aparecer un aviso explicando qué tipo de cookies utiliza la página, y pidiéndote **permiso** para usarlas.

Las opciones más habituales son:

- **Aceptar** todo, Estoy de acuerdo, Seguir adelante, Permitir todo... En este caso estamos aceptando el uso de todas las cookies.
- **Configurar**, Ajustar, Aceptar todas excepto..., Configurar cookies... Aquí nos permitirá ver y aceptar o rechazar los diferentes tipos de cookies.
- **Denegar**, No estoy de acuerdo, Rechazar... Pulsando en esta opción no nos enviarán cookies, pero en algunos casos la página web funcionará de manera distinta o no funcionará.

Fundación Telefónica

5 IDENTIFICACIÓN DE ESTAFAS

5. Identificación de estafas

Cada vez es más **frecuente** recibir mensajes engañosos a través de correo electrónico, SMS o WhatsApp, pero también a través de llamadas telefónicas.

Si sospechas que puede tratarse de un **fraude**, elimina inmediatamente el mensaje o abandona la llamada. **Ninguna entidad de confianza** te va a solicitar datos personales, números de cuenta o claves de acceso.

5.1. Tipos de estafa

Estos son los tipos más frecuentes de **estafa**:

- **PHISHING**
- **VISHING**
- **SMISHING**
- **WHATSAPP**

Las estafas pueden llegar por **cualquier vía**: teléfono, correo electrónico, WhatsApp... Incluso pueden llamar a la puerta de tu casa. Si alguna vez caes es una estafa, no te avergüences: **pide ayuda** y **denúncialo**.

PHISHING o "morder el anzuelo"

Son **mensajes que simulan** ser de una entidad **legítima**. Por ejemplo: un banco, la compañía de la luz, la Seguridad Social... Su finalidad es conseguir toda la información personal y bancaria que puedan.

Si caes en esta estafa:

- **Cambia** tus contraseñas.
- **Contacta** con tu entidad bancaria, en caso de haber facilitado este tipo de datos.
- Si has pulsado en algún enlace, pide **ayuda** para pasar un antivirus a tu dispositivo.
- **Advierte** a tu entorno, que no te dé vergüenza.

VISHING

Es muy parecido al phising, pero se lleva a cabo por **vía telefónica**, utilizando técnicas de ingeniería social. Un **supuesto operador** u **operadora** se identifica como empleada de una entidad de confianza, con objeto de obtener datos personales o dinero.

Estas técnicas suelen aprovechar la confianza, curiosidad, miedo o ignorancia de las personas.

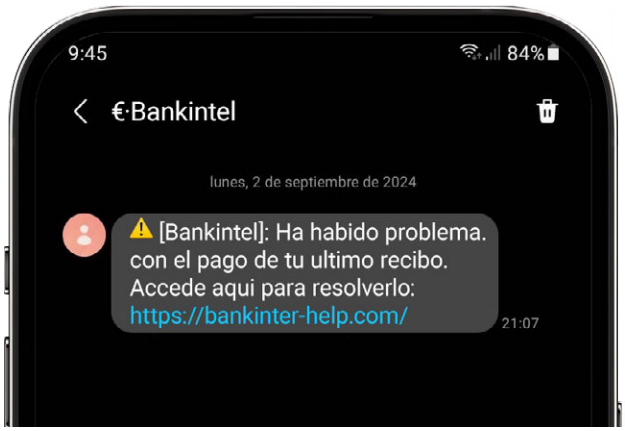
Si crees que una llamada puede ser vishing:

- **No proporciones** datos personales.
- **No cojas** llamadas extrañas.
- Aun si parece creíble lo que te hayan dicho, **es mejor colgar** y contactar tú con la entidad u organización, para verificar la información. No existen las ofertas increíbles ni te van a llamar exigiendo que pagues una multa.

SMISHING

En esta ocasión el intento de fraude llega a través de **SMS**, de nuevo simulando ser una entidad de confianza. Su objetivo es asimismo **robar información** o realizar un **cargo económico**.

Es muy común que el mensaje contenga un número para llamar (de tarificación especial) o un enlace de internet.

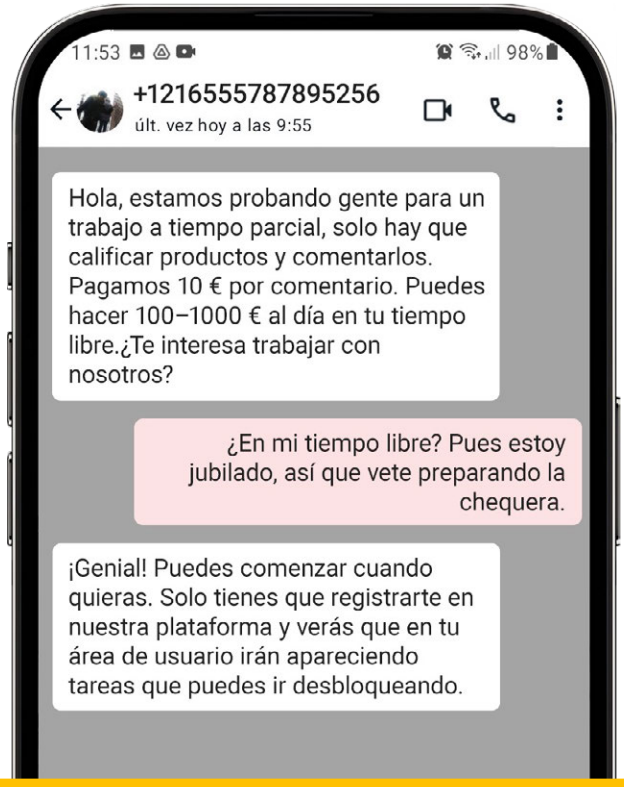


Si caes en esta estafa:

- Si has pulsado en algún enlace, pide ayuda para pasar un antivirus a tu dispositivo.
- Elimina cualquier archivo que hayas descargado.
- Contacta con tu entidad bancaria para cancelar pagos o la tarjeta.

WHATSAPP
(suplantación de identidad en redes sociales)

Suelen ser mensajes con un teléfono de **un país desconocido** y escriben por ejemplo "hola" para ver si pueden entablar conversación.
Te proponen **ofertas de trabajo** en nombre de empresas conocidas o pueden hacerse pasar por un **familiar en apuros**. El objetivo suele estar encaminado a obtener una ganancia económica.



¿Qué hacer si te abordan por WhatsApp?

- **No contestes**.
- **Bloquea el número**, verás la opción al abrir el mensaje en la parte inferior en Android (o superior en iOS).

5.2. Pautas para identificar estafas

Comprueba el remitente → Si es un número desconocido o un correo electrónico extraño, lo más probable es que sea un fraude.

Son frecuentes los errores ortográficos y gramaticales → Muchas veces son mensajes escritos con un traductor automático.

Analiza el asunto del correo electrónico → Suele ser llamativo: ofertas, alertas, etc.

Analiza el asunto del correo electrónico → Muchas veces son páginas web con nombres similares a los reales, para despistar (ej, bbbva.com o bbva-gestiones-online.com).
Las entidades de confianza nunca te enviarán enlaces sin haberlo solicitado tú. En todo caso te dirían que accedieras a su web o a tu área personal, pero sin proporcionarte ningún enlace.

Ten una actitud crítica con el objetivo del mensaje → ¿Qué es lo que quieren? Suelen solicitar una acción rápida y acotada en el tiempo.

Ten cuidado con los archivos adjuntos → Las entidades de confianza nunca te enviarán archivos sin haberlo solicitado tú (por ejemplo, si te das de alta en un servicio, pueden enviarte el contrato por email).

5.3. Dónde acudir

- **Asesoramiento**: INCIBE (Instituto Nacional de Ciberseguridad de España).

Teléfono **017**

WhatsApp **900 116 117**

Telegram **@INCIBE017**

- **Denuncias**: todas estas entidades tienen unidades de delitos telemáticos y pueden recoger denuncias en sus oficinas o por internet:

Policía Nacional

Guardia Civil

Ertzaintza

Mossos d'Esquadra

Policía Foral de Navarra

¡Gracias!

Notas

Notas

Créditos

Esta obra ha sido editada y coordinada por Fundación Telefónica.

Este contenido formativo puede incluir imágenes de marcas de terceros, y capturas de pantalla de aplicaciones tecnológicas, con fines exclusivamente didácticos y educativos, sin fines comerciales o lucrativos. Dichos elementos se muestran únicamente con el propósito de ilustrar conceptos y no implican afiliación, respaldo o asociación con los titulares de las marcas o desarrolladores de las aplicaciones reproducidas.

Todas las marcas comerciales y derechos de autor, en tales casos, pertenecen a sus respectivos titulares y propietarios. No existe ninguna relación comercial, de patrocinio o asociación de Fundación Telefónica con dichos titulares, salvo que se especifique expresamente.

Puedes acceder gratuitamente a los contenidos del proyecto Reconectados de Fundación Telefónica a través de este enlace:

https://www.fundaciontelefonica.com/voluntarios/reconectados/cursos-online/


Fundación
Telefónica