Fundación Telefónica

RECONECTADOS DIFUSIÓN

Ciberseguridad básica

GUÍA PARA EL FORMADOR

Índice

1. Introducción 4

1.1. Espacio de formación 4

1.2. Estructura de la sesión 4

2. En el aula 6

3. Material de apoyo 7

4. Ejercicios 8

5. En sesión 9

5.1. Tomando asiento y conociéndonos 9

5.2. Rompiendo el hielo 9

5.3. Comprobando el nivel 9

6. Comenzamos 10

6.1. ¿Qué es la ciberseguridad? 10

6.2. Gestión de contraseñas 11

6.3. Protección del dispositivo 13

6.3.1. Bloqueo de pantalla 13

6.3.2. Actualizaciones 15

6.3.3. Copia de seguridad 18

6.4. Navegación segura 20

6.4.1. Navegación privada o “modo incógnito” 21

6.4.2. Cookies 22

6.5. Identificar estafas 24

6.5.1. Tipos de estafa 24

6.5.2. Pautas para identificar estafas 27

6.5.3. Dónde acudir 28

1. Introducción

1.1. ESPACIO DE FORMACIÓN

El espacio donde se llevará a cabo la formación deberá estar acondicionado para el número de asistentes convocados.

Lo ideal es que disponga de:

- Wi-Fi al que poder conectarse.
- Pizarra con rotuladores como sistema de apoyo explicativo.
- Enchufes.
- Ordenador o, en su defecto, llevar ordenador portátil.
- Proyector.
- Pantalla proyectora o pizarra digital.
- Folios y bolígrafos.
- Mesas y sillas o sillas pupitre.

Es recomendable tener preparada una batería externa y llevar un USB con el material que necesitas, por si hay algún problema con la conexión a internet.

Dependiendo de las actividades que se elijan para la sesión, así como del número de asistentes, es recomendable preparar el aula para dividir al alumnado en grupos.

1.2. ESTRUCTURA DE LA SESIÓN

Aunque suponga un reto en su uso, las tecnologías e internet son un gran avance que nos facilitan actividades como encontrar información o comunicarnos.

No obstante, hay que ser consciente que el uso de internet también trae nuevas amenazas o situaciones que en mayor o menor medida implican un riesgo.

En este taller de 2 horas (120 min) se darán a conocer los riesgos y se aportarán herramientas para evitarlos y gestionar las situaciones más comunes.

Temas para trabajar

- Concepto de ciberseguridad.
- Gestión de contraseñas.
- Protección del dispositivo.
- Navegación privada y gestión de cookies.
- Identificación de estafas.

Objetivos generales

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

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

Cada grupo es diferente, deberás ajustar el temario (son epígrafes independientes unos de otros. El bloque tiene contenido suficiente para que no te quedes en blanco) **y los tiempos a las necesidades que se presenten en el aula. Lo importante es que lo que se trabaje en el taller sea entendido e interiorizado por los participantes, no acabar con el temario presentado.**

Al finalizar el taller, los asistentes dispondrán de una guía de consulta desde la que podrán acceder a todos los contenidos.

El **tiempo es estimado y variable**, según las necesidades del aula.

TEMA	TIEMPO (minutos)
Tomando asiento	5
Presentación	5
Testeo de nivel	5
Introducción a la ciberseguridad	10
Gestión de contraseñas	15
Protección de dispositivos	25
Navegación segura	20
Identificación de estafas	25
Dudas/Despedida	10

2. En el aula

Como dinamizador/a de la actividad:

- Dirígete al grupo con respeto.
- Mantén la escucha activa.
- Cuida tu lenguaje corporal.
- Adapta el vocabulario. No todas las personas entienden el lenguaje tecnológico. Es recomendable explicar o identificar qué significa cada palabra vinculada. Por ejemplo, ***icono*** («Los dibujos que tenéis en el móvil»). Esto no quiere decir que no se empleen estas palabras (de hecho, forma parte del aprendizaje), pero se deberán asociar siempre para que las interioricen.
- Pregunta si tu tono de voz es el adecuado. Algunas personas pueden tener problemas auditivos.
- Asegúrate de que se vea bien la pantalla en la que estás proyectando. Algunas personas pueden tener problemas visuales. En caso de dificultad, es recomendable explicar qué se está proyectando.
- Es posible que encuentres alguna persona que quiera monopolizar la sesión. Con serenidad, deberás desviar la atención que reclama esta persona y hacer partícipe al resto del grupo.
- No emplees expresiones como “esto es muy sencillo" o "fácil”.
- Reitera que estás para ayudar y que no deben tener vergüenza de intervenir.
- Emplea experiencias personales en los ejemplos para crear cercanía.
- Los gestos a la hora de explicar son fundamentales para que sigan las pautas. Por ejemplo, indica «1, 2, 3» con los dedos.

3. Material de apoyo

Además de esta guía, dispones de una presentación en Genially como apoyo para realizar la sesión en el aula.

Para que dicha presentación resulte útil es necesario que tengas en cuenta que:

Tienes anotaciones de ayuda que encontrarás repartidas por la presentación con el mismo icono en dos colores:

Azul: contiene información sobre los contenidos. Puede servirte de ayuda para recordar alguna explicación o alguna cuestión en la que debas insistir.

Naranja/Teja: contiene propuestas de dinámicas y sugerencias para trabajar las preguntas o realizar las prácticas.

- Es importante que recuerdes que el contenido de estos iconos **no ha de mostrarse en el aula,** únicamente se incluyen para que te sirvan a ti de ayuda cuando prepares la sesión y puedas repasar algunas cosas teniéndolos a mano. **Todo** lo que contienen está **más desarrollado en esta guía.**
- Repasa con los asistentes los iconos de navegación en Genially con la diapositiva correspondiente. Es conveniente que se familiaricen con ellos para que sean autónomos en el uso del material de autoaprendizaje. Importante: haz este repaso al final de la sesión, ya que desvía la atención y consume tiempo de la sesión.

4. Ejercicios

La sesión formativa debe constar de una **parte explicativa** (para la que dispones de un Genially como material de **apoyo**) y de una **parte práctica**.

Para desarrollar la **parte práctica** se presenta una batería de ejercicios que encontrarás **al final de esta guía**, para realizar a nivel individual y grupal.

Selecciona las prácticas en función de si van a ser individuales o grupales, así como de las necesidades del aula, el apoyo con el que cuentes y el tiempo disponible.

Aunque trabajes en grupo, debes llevar a cabo también **ejercicios individuales**.

En grupo

Las dinámicas de grupo te servirán para fomentar la participación.

Para trabajar de forma grupal es **importante** que puedas **preparar la sesión previamente** (en materiales y presentaciones), cuando ya conoces el número de personas del grupo y sabes con qué materiales cuentas.

Para que todos/as prueben y practiquen lo aprendido con su dispositivo, te recomendamos que organices los tiempos y las intervenciones del aula:

1. Primero explica un apartado del temario.
2. Resuelve las dudas que hayan surgido.
3. Realiza ejercicios con sus dispositivos.

De esta manera asignas un espacio en la sesión para los distintos ejercicios, garantizas que tienes toda la atención de tus alumnos durante la explicación y puedes resolver las dudas concretas y avanzar con el temario siguiendo los ritmos del alumnado.

Siempre que se pueda trabajar en grupo, será más dinámico y ameno para los participantes. Por contra, **deberás estar muy atento/a para gestionar los tiempos y los grupos**. Es fundamental que, si se eligen actividades en grupo de puesta en común, se nombre un portavoz de grupo.

Igualmente, **para finalizar la sesión** formativa puedes elegir alguna de las preguntas de cada bloque y emplearlo a modo de repaso, o trabajar en el caso global que se presenta en el anexo de actividades.

¡Recuerda, son propuestas! Puedes realizar otros ejercicios relacionados con el tema si lo consideras oportuno. Igualmente, no tienes por qué hacer todos.

5. En sesión

5.1. TOMANDO ASIENTO Y CONOCIENDO QUIÉNES SOMOS

Si es posible mira mientras se sientan los dispositivos que traen, para **detectar** los sistemas operativos y marcas, ya que en muchos casos no van a saber contestar si lo preguntas. Cada sistema, versión y modelo serán distintos, pero tener una idea de lo que hay en el aula te permite hacer alusiones directas, sobre todo en caso de **peculiaridades** en las marcas.

5.2. ROMPIENDO EL HIELO

- Preséntate y presenta a los compañeros o compañeras que estén contigo.
- Presentación de participantes si hay un número reducido (5-7).
- Pregunta cuáles son sus expectativas.
- Explica cómo va a funcionar la sesión:
    - Explicamos.
    - Participamos.
    - Prácticas con sus dispositivos.

5.3. COMPROBANDO EL NIVEL

Es necesario comprobar el nivel del aula para poder adecuar la formación. Esto se hará a través de preguntas, escuchando las respuestas y observando a los asistentes.

En el caso de esta formación, es posible que muchos de los asistentes deseen tener un primer acercamiento a la banca digital, más que empezar a usarla de forma inminente. **Es importante determinar sus expectativas.**

Algunos ejemplos que puedes utilizar:

- ¿A qué os suena la ciberseguridad?
- ¿Creéis que podemos hacer algo para proteger nuestros dispositivos? ¿El qué?
- ¿Tenéis configurada alguna medida de seguridad en vuestros teléfonos? ¿Cuál?
- ¿Actualizáis vuestros teléfonos y aplicaciones? Es posible que muchos asistentes no lo hagan. Pregunta por qué. En muchos casos será por miedo a lo que pueda suceder o por falta de espacio en el dispositivo.

La escucha activa es verdaderamente importante, así como dar respuesta a las preguntas o inquietudes que se planteen en cada momento. Si hay algo que se verá más adelante, a lo largo de la sesión, lo diremos.

6. Comenzamos

Lleva a cabo una breve introducción indicando las ventajas de internet y los riesgos que supone. Traslada que es **normal que las personas tengan miedo**, inseguridad o se sientan amenazadas.

Traslada de **forma positiva** al aula que lo importante es conocer los riesgos y saber qué hacer para evitar situaciones desagradables; **este es el fin del taller**.

6.1. ¿QUÉ ES LA CIBERSEGURIDAD?

Aunque los términos *ciberseguridad* y *ciberataque* nos suenan a algo que afecta a grandes organizaciones, la realidad es que nos impacta a todos, desde las empresas a los ciudadanos de a pie. Podemos protegernos siguiendo consejos como los que vamos a trabajar y utilizando el sentido común.

Se entiende por **ciberseguridad** a *las prácticas que llevamos a cabo para proteger nuestros ordenadores y dispositivos móviles de posibles riesgos mientras navegamos por la red.*

> ¡Ojo! En este punto, es importante transmitir que nuestros teléfonos y ordenadores, aunque no los estemos usando, **están conectados a internet**.

¿Qué es un **ciberataque**? Una acción intencionada llevada a cabo con objeto de robar, exponer o destruir datos a través de un acceso no autorizado a nuestros dispositivos.

Una vez expuesta la definición de los términos más generales, avanza para dar a conocer las herramientas de las que disponemos para poder protegernos.

Reflexiona

¿Crees que la ciberseguridad o los ciberataques nos afectan a todos nosotros?

¿O es por el contrario un tema que afecta 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...

¿Dejarías abierta la puerta de tu casa cuando te vas de vacaciones?

6.2. GESTIÓN DE CONTRASEÑAS

Las contraseñas son uno de los primeros mecanismos de defensa que tenemos para ayudar a proteger nuestros datos.

Ejemplo: para entrar a nuestra casa necesitamos la llave para abrir la puerta. Esa llave sería nuestra contraseña.

Por tanto, podemos decir que 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 nuestro teléfono.

> ¡Ojo! Las contraseñas deben ser **secretas**.

Ya que se ha mencionado el ejemplo de la puerta y la llave, usa el símil para hacer ver que existen contraseñas débiles y robustas. Ejemplo: si la llave y la puerta son blindadas serán más seguras que una puerta antigua de cierre sencillo.

Crear una contraseña segura

La mayoría de los asistentes utilizarán la misma contraseña en todos los servicios para no olvidarse de ella. Es importante transmitir que, aunque es comprensible, no debería ser así. Si usamos la misma para todo y alguien la roba, el ladrón tendrá acceso a todas nuestras cosas. Una contraseña debe ser relativamente **simple**, para poder recordarla, pero a la vez **segura**. Por ejemplo:

- Evita fechas de nacimiento y otros detalles personales.
- Evita contraseñas comunes, como 12345.

Ten en cuenta que el cambio de hábitos no va a llegar de manera inminente, pero si se presentan alternativas, lo más probable es que reflexionen y hagan pequeñas modificaciones en sus costumbres.

> ¡Ojo! Algunos servicios o aplicaciones pueden limitar la composición de la contraseña (mayor o menor longitud, sin espacios en blanco, etc.). En ese caso, es recomendable combinar la mayor variedad posible dentro de las posibilidades permitidas, incluyendo minúsculas, mayúsculas, números y símbolos.
>
> Por ejemplo: 4yU_*so7)@N¡

En la actualidad, se recomienda utilizar un conjunto de palabras (passphrase) con al menos 16 caracteres. Se puede 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, y añade alguna variación para no resultar demasiado predecible:

¡Houston, tenemos 2 problemas!

Una estrategia posible para poder recordar muchas contraseñas es crear una estructura que tenga una parte fija (la contraseña base) a la que se añade por ejemplo el nombre del servicio y algún número o símbolo (ej, la longitud del nombre del servicio y un guion separador).

Ejemplo: Gmail5 - pardos gatos abundan
Unicaja7 - pardos gatos abundan
Amazon6 - pardos gatos abundan

Aun así, muchos servicios y aplicaciones restringen la longitud y la composición de la contraseña (por ejemplo, no admiten espacios en blanco o limitan la longitud a 12 caracteres). En este caso, puede ser imposible recordar todas las contraseñas que tenemos sin ayuda.

Menciona que podemos acudir a un **gestor de contraseñas**, que es una aplicación que sirve para almacenarlas en un formato seguro, imposible de descifrar. Es como apuntarlas en un cuaderno que solo tú puedes leer.

Hay gestores de contraseñas gratuitos (ej: KeePass) y otros gratuitos, con versión de pago para acceder a funcionalidades extra (ej: EnPass, 1Password, Bitwarden).

También puedes mencionar que los **navegadores** suelen llevar incluida la función de **recordar contraseñas** y cuando accedes a un sitio suelen preguntarte si quieres recordar los datos de acceso para facilitártelo la próxima vez. Esta es una buena ayuda en muchas ocasiones, aunque es recomendable no almacenar credenciales para sitios o servicios que contengan información confidencial. Las web de los bancos y las que contienen datos médicos o fiscales suelen tener sistemas de protección para evitar que pueda almacenarse la información de acceso, evitando así posibles problemas de seguridad.

PRÁCTICAS

Apartado 2.2. Anexo Ejercicios. Preguntas grupales.

Individuales. Piensa en una contraseña que tengas. Con lo que ahora sabes, ¿crees que es segura? Con todo lo aprendido, piensa una contraseña segura. Evalúa la seguridad de tu contraseña en un servicio de validación. P. ej: https://password.kaspersky.com/es/

6.3. PROTECCIÓN DEL DISPOSITIVO

Es un buen momento para reflexionar y pensar para qué usamos el móvil y qué información tenemos guardada: contactos, mensajes de citas sanitarias, fotografías... De esta manera se puede advertir la necesidad de tener el teléfono con la pantalla bloqueada.

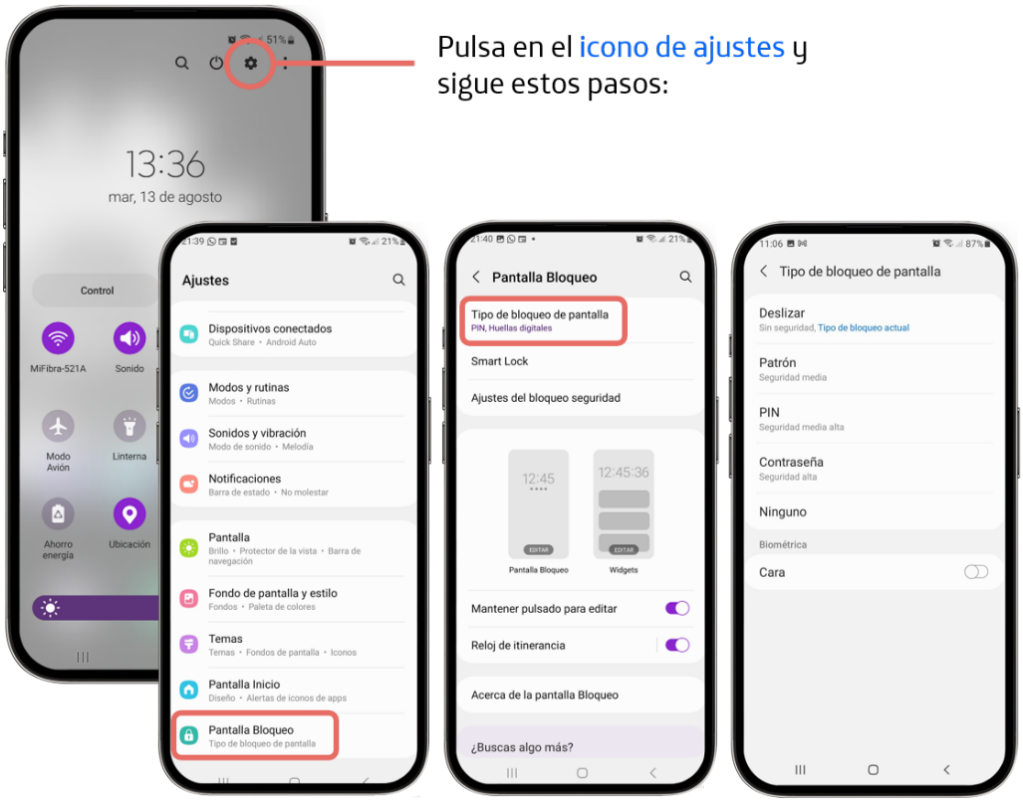
Ejemplo: si te roban el teléfono en la calle y no tiene ningún tipo de protección de bloqueo, el malhechor o malhechora puede acceder a toda la información que tienes guardada.

Dependiendo del nivel que hayas detectado en el grupo, puedes también hablar de lo importante que es tenerlo bloqueado si usan el móvil para pagar (NFC), ya que se necesita desbloquear el móvil para llevar a cabo el pago. Pregunta en qué otras ocasiones creen que es importante que el móvil esté bloqueado.

6.3.1. BLOQUEO DE PANTALLA

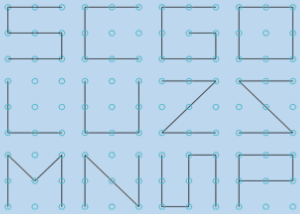
Da a conocer los tipos de bloqueo de pantalla y en qué consiste cada uno a través de imágenes.

> ¡Ojo! Hay que tener en cuenta que puede haber variaciones, dependiendo de cada modelo y versión de sistema operativo.

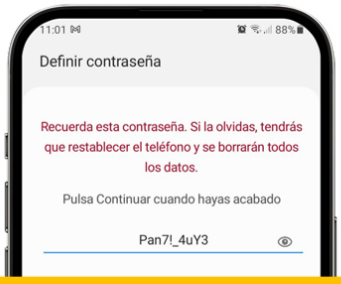


Tipos de bloqueo de pantalla

- 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.

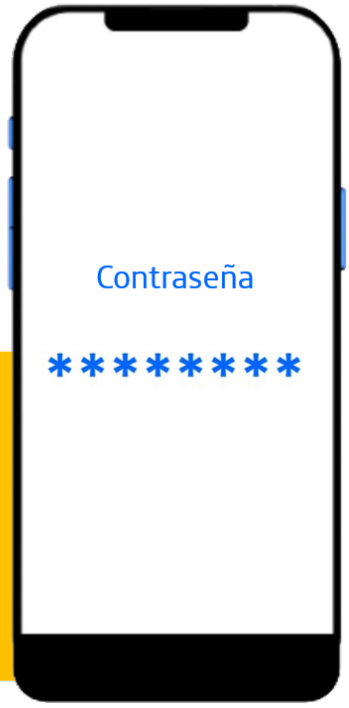


- Usar 8 puntos de manera aleatoria permite crear un patrón seguro.



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.



PRÁCTICAS

Individuales. ¿Tienes bloqueada la pantalla del teléfono? En caso de no estarlo, ¿te animas a practicar y bloquearla?

6.3.2. ACTUALIZACIONES

Como se comentaba al principio, hay un porcentaje significativo de personas mayores que **no actualizan**, sobre todo el sistema operativo. Esto es debido al **miedo** o el **desconocimiento**; también puede influir la falta de espacio en el dispositivo.

Los sistemas operativos, así como las aplicaciones de nuestro teléfono pueden tener **fallos de seguridad**; este es un motivo importante por el hacen falta las actualizaciones.

"Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad." (INCIBE)

Las actualizaciones son **necesarias para tener protegido el dispositivo**,

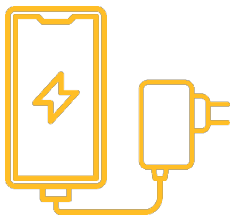
Para estar tranquilos, se recomienda en general:

- Elegir la actualización automática si está disponible.
- Instalar las actualizaciones lo antes posible.
- Actualizar las aplicaciones siempre desde la tienda oficial (Play Store en Android, App Store en iOS).

Actualizaciones del sistema operativo

El sistema operativo es el programa más importante de tu dispositivo, el que hace que funcione el teléfono. Te permite usarlo y darle órdenes para que haga lo que necesitas. Los más comunes son Android y iOS (iPhone).

Las actualizaciones del sistema operativo son **fundamentales para aumentar la seguridad**, ya que subsanan errores e incluyendo nuevas mejoras y funcionalidades. Los fabricantes recomiendan que se apliquen lo antes posible.



Para realizar las actualizaciones el teléfono debe estar enchufado a la red y conectado a una red Wi-Fi, para evitar gastar datos (pueden ser actualizaciones de gran tamaño) y quedarse sin batería a la mitad de la actualización.

Advertencia: esto no se hace durante la formación.

Una vez más, hay que tener en cuenta las marcas y versión del sistema operativo, ya que los fabricantes suelen tener sus propias versiones de Android, ajustadas a las necesidades de cada dispositivo. La localización de la función de actualización puede variar. Estas son algunas de las más frecuentes:

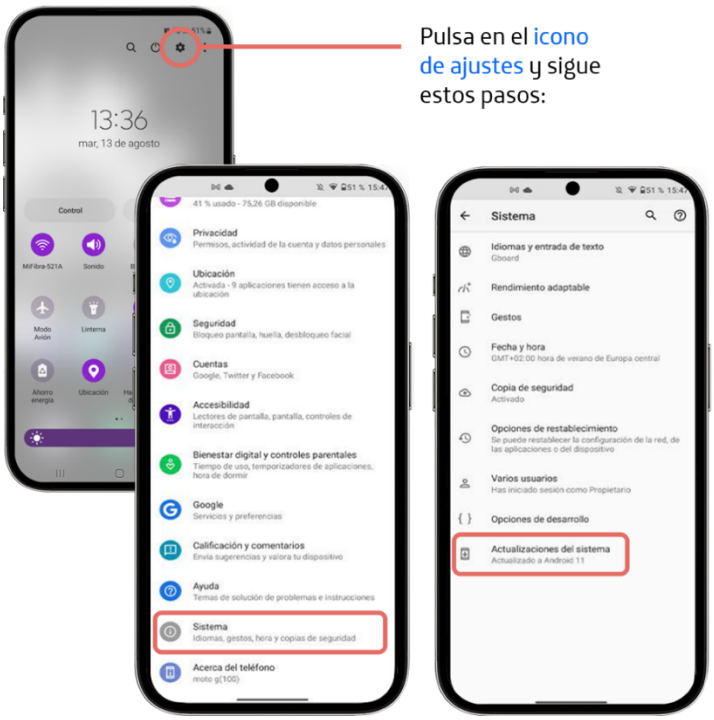
Ajustes → Actualización de software (o del sistema)

Ajustes → Sistema → Actualización de software

Ajustes → Sistema → Ajustes avanzados → Actualización de software

Ajustes → Información del teléfono (o Sobre el teléfono) → Actualizaciones del sistema

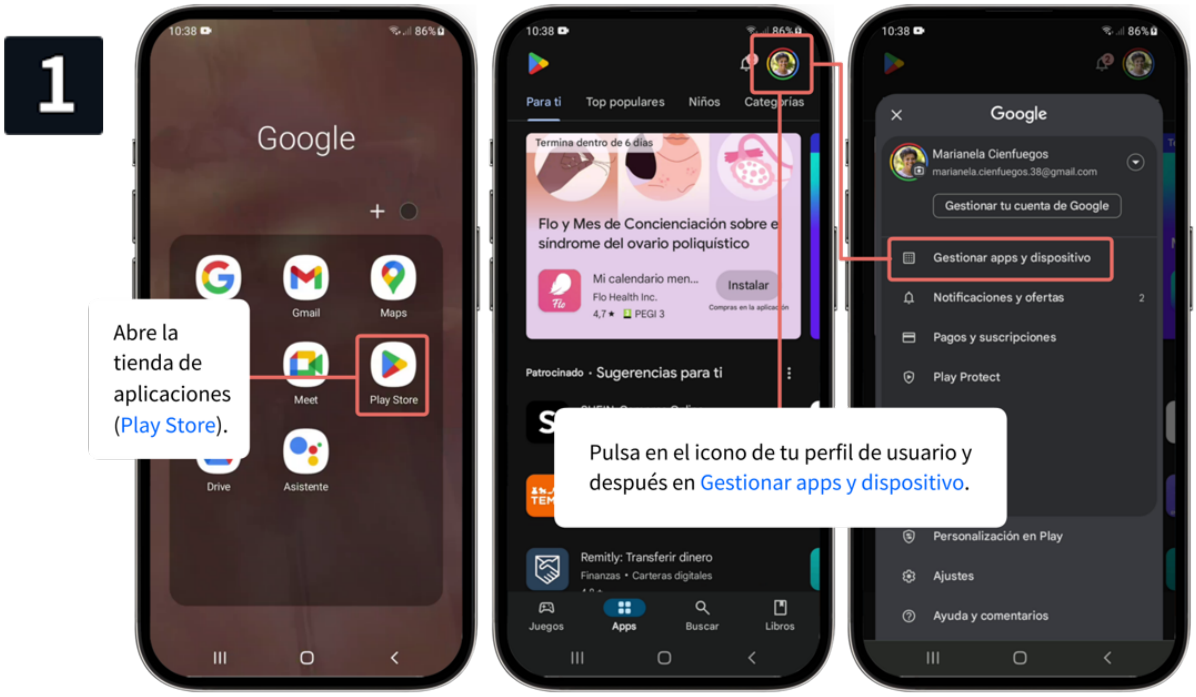
Ajustes → General → Acerca del teléfono → Actualizar SW

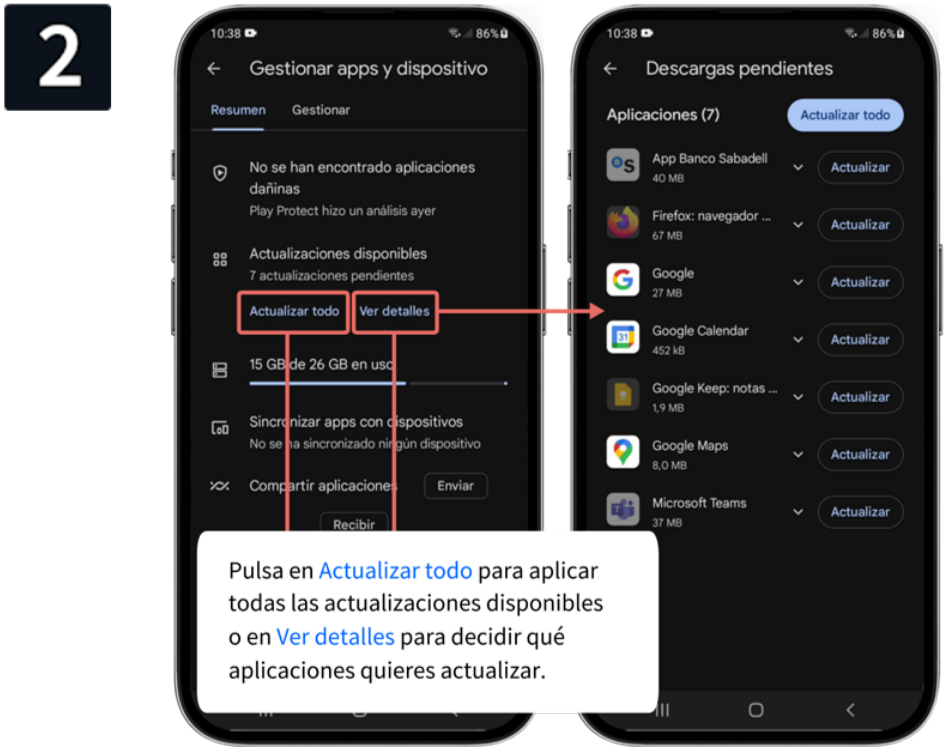


Actualizaciones de aplicaciones

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...

Al igual que en el caso de los sistemas operativos, actualizar las aplicaciones permite acrecentar la seguridad y obtener mejoras y nuevas funcionalidades.





6.3.3. COPIA DE SEGURIDAD

Habitualmente, las personas mayores **no crean copias de seguridad**, y en caso contrario suele ser porque ha sido configurado por un familiar o amigo.

La incertidumbre y desconfianza de que sus datos están en internet es una realidad. Habla de **lo importante que es crear una copia de seguridad** para no perder los datos.

A la hora de instalar una actualización del sistema es recomendable hacer una copia de seguridad previamente.

Pregunta si han oído hablar de esta función y por qué creen que es necesaria.

Una copia de seguridad es un duplicado de los datos personales que se ubica en un lugar seguro de internet. Puede utilizarse ese duplicado para restaurar la información en un teléfono nuevo. Esta copia puede hacerse de manera automática.

¿Por qué hay que crear una copia de seguridad?

- Para conservar los datos del teléfono.
- Para tener mayor facilidad a la hora de poner en marcha un nuevo teléfono.
- Para no perder la información.

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

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

La copia de seguridad de **fotos y vídeos** se hace a través de Google Fotos y funciona igual. La diferencia es que si se elimina una foto por error, antes de eliminarse para siempre permanecerá durante 30 días en la papelera, tanto en el 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.

Qué se necesita para hacer una copia de seguridad

Gmail

Correo electrónico de Google:
xxxxx@gmail.com

Google Drive

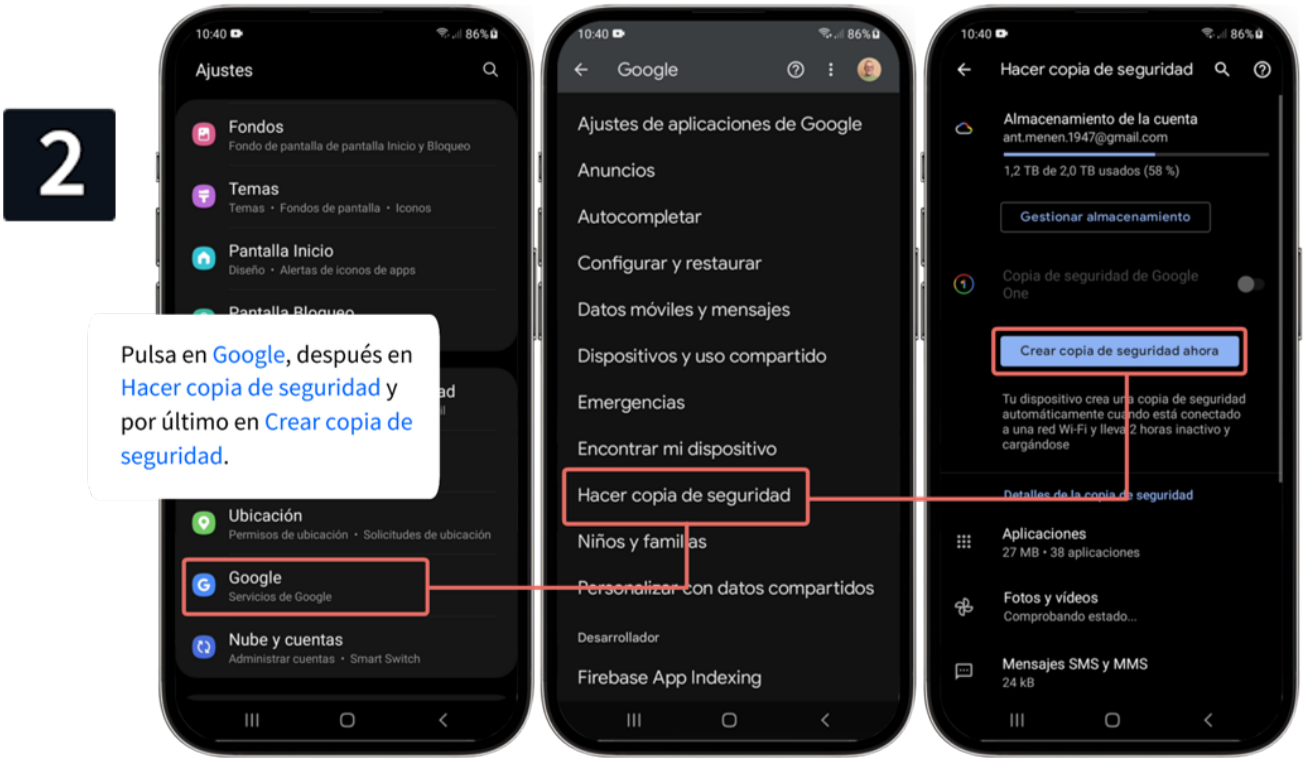
Plataforma de almacenamiento de datos en la nube.

Cuando se pone en marcha un teléfono móvil inteligente, debe usarse o abrirse una cuenta nueva de correo electrónico. Las cuentas de Google (xxxxx@gmail.com) vienen con 15 GB de almacenamiento gratuito. Si alguien necesita más espacio, existen distintos planes de pago en su servicio Google One.

Para hacer la copia:

1

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



PRÁCTICAS

Individuales. Haz una copia de seguridad.

Si no quieres la copia, después puedes desactivar la función y eliminar la copia desactivando la Copia de seguridad de Google One en el mismo sitio.

6.4. NAVEGACIÓN SEGURA

Para introducir este apartado, es conveniente saber si los asistentes conocen **la diferencia entre navegador y buscador**.

Introduce los conceptos.

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

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

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/

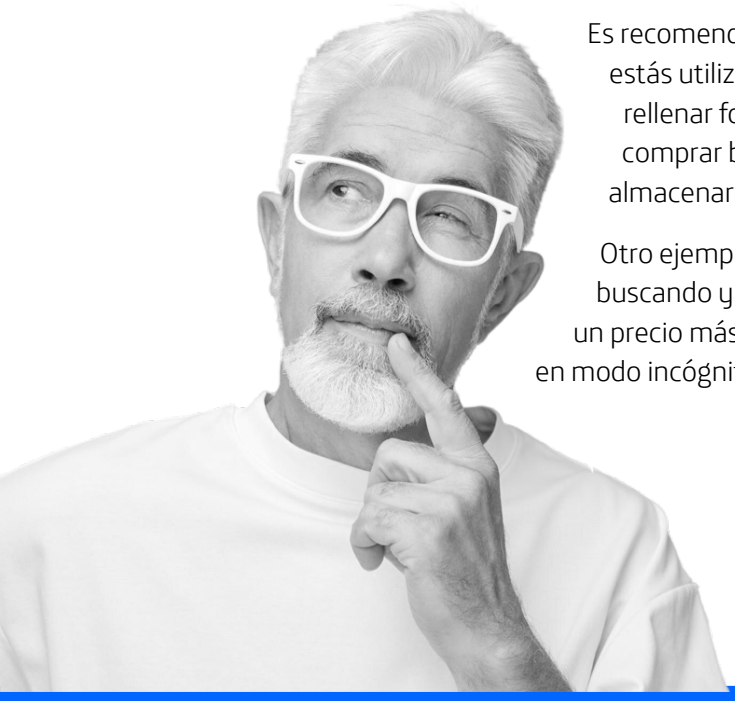
Cada vez que buscamos algo en internet, vamos dejando rastro de lo que hacemos.

En ocasiones es importante navegar de la manera más segura y privada posible. A continuación veremos cómo.

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...

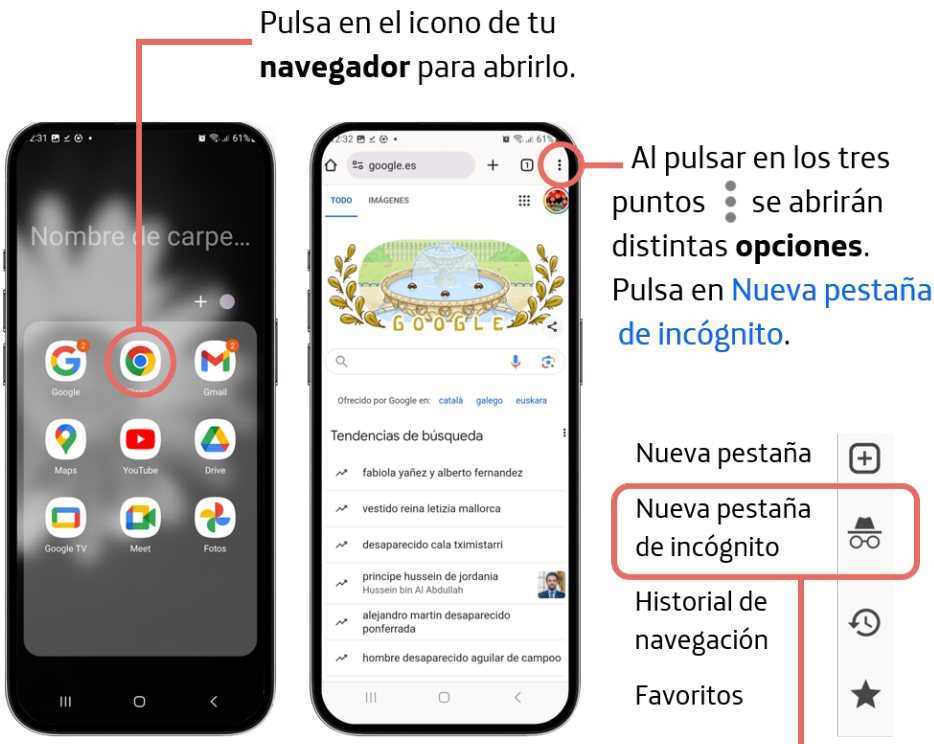
6.4.1. NAVEGACIÓN PRIVADA O "MODO INCÓGNITO"

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.



6.4.2. COOKIES

Las cookies es un tema que suele resultar algo confuso. Explica que son pequeños ficheros de datos que envían las páginas web que visitan en el teléfono u ordenador. No son malas *per se*, aunque sus funcionalidades suelen aprovecharse en el ámbito comercial.

Ejemplo: hemos buscado unas botas de montaña para comprar; empezaremos a ver en nuestro navegador publicidad relacionada con esta búsqueda.

Las cookies no son el único "truco" que emplean los programadores como método de seguimiento del usuario. También puede utilizarse la IP, la huella del navegador o el dispositivo, los *beacon* (o píxeles transparentes), etc.

Las cookies tienen múltiples utilidades:

- **Facilitar la navegación** por las páginas web.
- **Recordar información**: nuestra identidad, preferencias al visitar una web, lo que hay en nuestra cesta de la compra, etc.
- **Analizar nuestras actividades** y comportamiento. Esto último es lo que puede servir para enviarnos información relacionada con tus intereses.

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

Con independencia de las cookies que quieran enviar las páginas web, puede indicarse al navegador que las bloquee buscando en su sección de 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 pueden bloquearse las cookies desde el navegador de forma generalizada, conviene revisar las políticas de cookies y privacidad de las páginas web, ya que existen diferentes técnicas de rastreo que nada tienen que ver con las cookies. Algunos navegadores incluyen preferencias en el apartado de Privacidad para protegerse de algunas de esas técnicas (que hemos mencionado antes).

Hay que tener en cuenta que algunas cookies son necesarias y no pueden desactivarse si queremos que funcione la página web (por ejemplo, en la web de un supermercado, si las usan para recordar los productos que queremos comprar). Para **gestionar las cookies** hay algunas opciones comunes.

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.

PRÁCTICAS

Apartado 2.4. Anexo Ejercicios. Preguntas grupales.

Individuales. Abre el navegador en modo incógnito y busca información sobre ciberseguridad. Busca una página web de un medio de comunicación. Reflexiona sobre las cookies que presenta y gestiónalas. Buscar una página web de un comercio. Reflexiona sobre las cookies que presenta y gestiónalas.

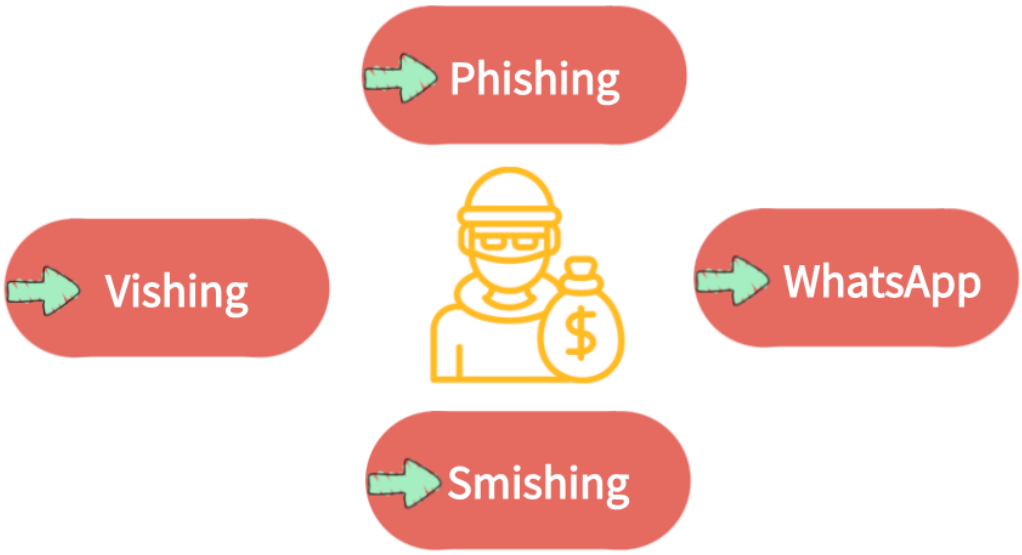
6.5. IDENTIFICAR ESTAFAS

Cada vez hay más información y las personas están más **sensibilizadas** con esta cuestión, y este es un tema que nos preocupa a todos.

Sabemos que es frecuente recibir mensajes por correo electrónico o SMS con fines de engaño, pero también sucede a través de llamadas telefónicas.

Transmite que, en caso de sospechar de un fraude **nunca se deben seguir las indicaciones que nos den**; además, hay que interiorizar que **ninguna entidad** va a solicitar datos personales, números de cuenta o claves de acceso.

Lo importante, en este caso, no es tanto el nombre que se le da a cada tipo de estafa, sino la identificación de posibles riesgos.



6.5.1. TIPOS DE ESTAFA

Phishing

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 eres víctima de un phishing

- 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.

En caso de haber "mordido el anzuelo" y haber pulsado en enlaces o descargado ficheros maliciosos, conviene pasar un antivirus al dispositivo. Es conveniente que pidan ayuda a alguien de su confianza para hacerlo, ya que este es un tópico avanzado: hay que saber qué antivirus son más recomendables y cómo configurarlos y ejecutarlos.

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.

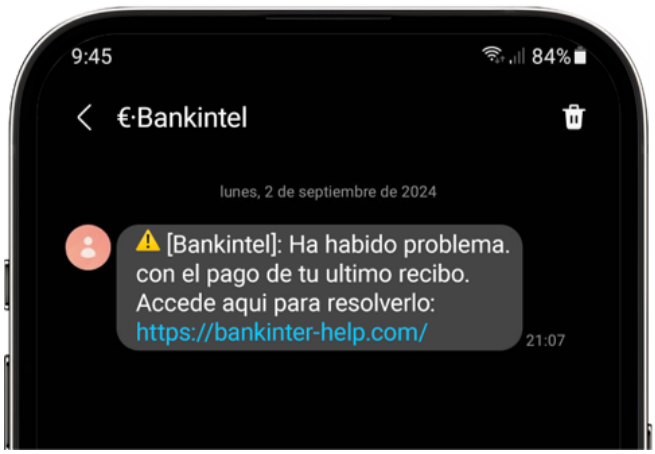
Estas técnicas suelen aprovechar la confianza, curiosidad, miedo o ignorancia de las personas.

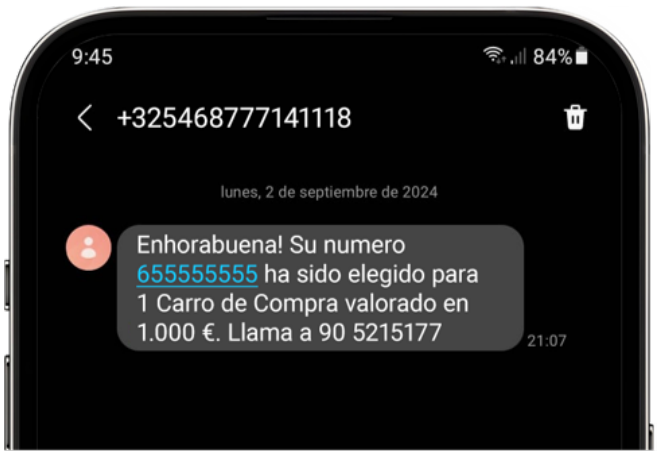
Si crees que una llamada puede ser vishing:

- 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.



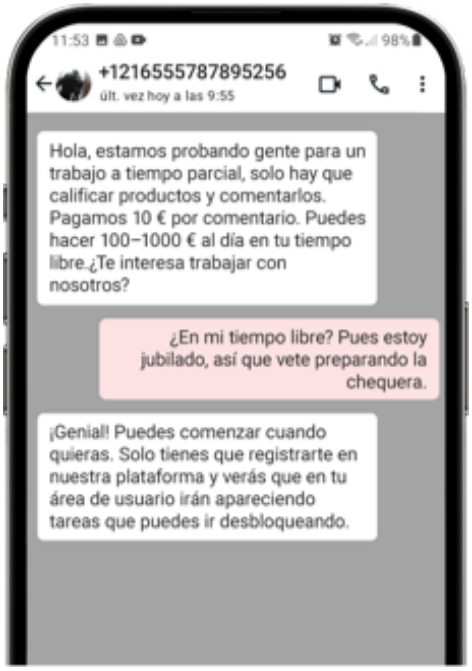


Si caes en esta estafa:

- 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).

6.5.2. PAUTAS PARA IDENTIFICAR ESTAFAS

Si bien hay una serie de pautas y consejos que se van a proporcionar, lo primero que se debe hacer es **mantener la calma** y utilizar el **sentido común**. Explica que, aunque el mensaje haya llegado, no hay ningún riesgo, siempre y cuando no se haya abierto el enlace o documento adjunto a veces contienen estos mensajes.

Se deberá:

- **Comprobar el remitente**. Si es un número desconocido o un correo electrónico extraño, lo más probable es que sea un fraude..
- Se **analizará el asunto del correo electrónico**. Suele ser llamativo: ofertas, alertas, etc.
- Hay que ser **críticos con el objetivo del mensaje** y preguntarse qué es lo que quieren. Suelen solicitar una acción rápida y acotada en el tiempo.
- Es **frecuente encontrar errores ortográficos y gramaticales**. Muchas veces son mensajes escritos con un traductor automático.
- **Observar el enlace antes de pulsar en él**. Muchas veces son páginas web con nombres similares a los reales, para despistar (ej, bbva-gestiones-online.com o bbbva.com). Las entidades de confianza nunca enviarán enlaces sin haberlo solicitado. En todo caso, nos dirían que accediéramos a su web o a nuestra área personal, pero sin proporcionar ningún enlace.
- **Ser cuidadosos con los archivos adjuntos**. Las entidades de confianza nunca te enviarán archivos sin haberlo solicitado nosotros (por ejemplo, si nos acabamos de dar de alta en un servicio, nos pueden enviar el contrato por email).
- **Emplear el sentido común**.

6.5.3. 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

PRÁCTICAS

Apartado 2.5. Anexo Ejercicios. Preguntas grupales.

Individuales. Busca información sobre las cadenas de WhatsApp. ¿Qué son? ¿Alguna vez has recibido alguna? ¿Qué deberías hacer si te llega una?

NOTAS:

CRÉDITOS

Esta obra ha sido editada y coordinada por Fundación Telefónica.

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

RECONECTADOS

Fundación Telefónica

RECONECTADOS

Ciberseguridad básica

GUÍA PARA EL FORMADOR: PROPUESTA DE EJERCICIOS

Índice

1. Introducción **3**

2. Propuesta de ejercicios **5**

2.1. Qué es la ciberseguridad (Guía formador apartado 6.1.) 5

2.1. Gestión de contraseñas (Guía formador apartado 6.2.) 7

2.2. Protección del dispositivo (Guía formador apartado 6.3.) 8

2.3. Navegación segura (Guía formador apartado 6.4.) 10

2.4. Identificar estafas (Guía formador apartado 6.5.) 11

3. Caso global para trabajar **14**

4. Solucionario **15**

1. Introducción

La sesión que se va a impartir se compone de una parte explicativa con material de apoyo proyectado, y además tiene que ir acompañada con ejercicios prácticos que permitan al alumnado interiorizar lo explicado.

A continuación se presenta una propuesta de posibles actividades que puedes realizar con los asistentes. Deberás **seleccionarlas** teniendo en cuenta si trabajas en dinámica grupal o individual. También tendrás en cuenta los tiempos que se vayan estableciendo, según el nivel del aula.

Aunque trabajes en grupo, debes plantear también **ejercicios individuales**.

Las dinámicas de grupo te servirán para fomentar la participación. En caso de no poder realizar grupos, se pueden lanzar las preguntas para que los participantes respondan.

En grupo

Para trabajar de forma grupal es **importante** que puedas **preparar la sesión previamente** (en materiales y presentaciones), cuando ya conoces el número de personas del grupo y sabes con qué materiales cuentas.

Para que todos/as prueben y practiquen lo aprendido con su dispositivo, te recomendamos que organices los tiempos y las intervenciones del aula:

1. Primero explica un apartado del temario.
2. Resuelve las dudas que hayan surgido.
3. Realiza ejercicios con sus dispositivos

De esta manera asignas un espacio en la sesión para los distintos ejercicios, garantizas que tienes toda la atención de tus alumnos durante la explicación y puedes resolver las dudas concretas y avanzar con el temario siguiendo los ritmos del alumnado.

Siempre que se pueda trabajar en grupo, será más dinámico y ameno para los participantes. Por contra, **deberás estar muy atento/a para gestionar los tiempos y los grupos**. Es fundamental que, si se eligen actividades en grupo de puesta en común, se nombre un portavoz de grupo.

Además de trabajar con los ejercicios del material de apoyo, también puedes trabajar con material de papelería para desarrollar la parte de actividades (muy útil si te encuentras en un espacio con problemas de conexión a la red).

Cada equipo tendrá en su mesa folios y bolígrafos, además de rotuladores de colores.

La propuesta de colores puede cambiarse. Además del color, es interesante que introduzcas el elemento del dibujo. Por ejemplo:

- En azul, que pinten un check.
- En rojo, que pinten una "X".

También puedes:

- Imprimir las preguntas-respuestas y que marquen en el papel.
- Que escriban en papel (esto es algo más tedioso).

Las actividades se presentan en bloques en los que estamos trabajando. Te recomendamos que en el caso de las actividades grupales, las vayas introduciendo a medida que avanzas en un tema.

Dentro de cada bloque se presentarán las propuestas en este orden:

1. Preguntas grupales.
2. Ejercicios individuales.

En el último apartado de esta guía (Solucionario) se encuentran todas las soluciones a las preguntas grupales.

Igualmente, **para finalizar la sesión** formativa puedes elegir alguna de las preguntas de cada bloque y emplearlo a modo de repaso, o trabajar en el caso global que se presenta en el anexo de actividades.

¡Recuerda, son propuestas! Puedes realizar otros ejercicios relacionados con el tema si lo consideras oportuno. Igualmente, no tienes por qué hacer todos.

2. Propuestas de ejercicios

2.1. QUÉ ES LA CIBERSEGURIDAD (guía del formador, apartado 6.1.)

Preguntas grupales

1. **¿Es necesario tener profundos conocimientos de informática para poder protegerte de los ciberataques?**

   a) Sí.

   b) No.

2. **Cuando los dispositivos están en reposo con la pantalla apagada, no están conectados a internet.**

   a) Sí, siguen conectados a internet por eso es importante tomar medidas de seguridad.

   b) No, no están conectados porque están modo reposo, para que se conecten debemos desbloquearlos.

2.2. GESTIÓN DE CONTRASEÑAS (guía del formador, apartado 6.2.)

Preguntas grupales

3. **¿Cuál de estas pautas es más indicada para crear una contraseña robusta?**
   a) 5-8 caracteres + mayúsculas + números + signos.
   b) Más de 15 caracteres.
4. **¿Cuál de estos dos ejemplos es una contraseña más robusta?**
   a) &Reconectados2024
   b) &Reconectados*2024
5. **¿Es adecuado utilizar la misma contraseña para todo?**
   a) Sí, porque así se recuerda mejor.
   b) No, es mejor tener una para cada cosa.

Ejercicios individuales

- Piensa en una contraseña que tengas. Con lo que ahora sabes, ¿crees que es segura?
- Con todo lo aprendido, piensa una contraseña segura.
    - Evalúa la seguridad de tu contraseña en un servicio de validación, por ejemplo: https://password.kaspersky.com/es/

2.3. PROTECCIÓN DEL DISPOSITIVO (guía del formador, apartado 6.3.)

Ejercicios individuales

- ¿Tienes bloqueada la pantalla del teléfono? En caso de no estarlo, ¿te animas a practicar y bloquearla?
- Comprueba si tienes aplicaciones pendientes de actualizar.
    - Puedes actualizarlas una a una, o todas juntas.
    - Recuerda que para hacerlo debes estar conectado a una red Wi-Fi de confianza o disponer de datos suficientes.
- Haz una copia de seguridad.
    - Si no quieres la copia, después puedes desactivar la función y eliminar la copia desactivando la Copia de seguridad de Google One en el mismo sitio.

2.4. NAVEGACIÓN SEGURA (guía del formador, apartado 6.4.)

Preguntas grupales

1. **Completa la frase: "Un ... es la aplicación que permite acceder a internet".**
   a) Navegador.
   b) Buscador.
2. **La navegación de incógnito sirve:**
   a) Para que las páginas web que visitamos no queden registradas.
   b) Para que queden registradas las búsquedas que hacemos y las web que visitamos.
3. **Las cookies solo sirven para conocer tus hábitos de navegación.**
   a) No, también vale para recordar los accesos.
   b) Sí, por eso luego nos sale publicidad de lo que buscamos.
4. **¿Dónde pulsarías para escoger las cookies que quieres aceptar?**
   a) Aceptar todas.
   b) Configurar cookies.

Ejercicios individuales

- Abre el navegador en modo incógnito y busca información sobre ciberseguridad.
- Busca una página web de un medio de comunicación. Reflexiona sobre las cookies que presenta y gestiónalas.
- Buscar una página web de un comercio. Reflexiona sobre las cookies que presenta y gestiónalas.

2.5. IDENTIFICAR ESTAFAS (guía del formador, apartado 6.5.)

Preguntas grupales

1. ¿Qué tipo de estafa es esta?

a) Phishing.

b) Smishing.

c) Vishing.

d) No es una estafa.

2. Recibes una llamada telefónica de una persona que trabaja en una empresa energética con la que ya no tienes ningún contrato. Hace meses que tienes el suministro con otra empresa. Tras identificarse, te empieza a hacer preguntas:
—¿Estoy hablando con (aquí dice tu nombre y tus apellidos)?
—¿Me podría confirmar que vive usted en la calle (aquí dice tu domicilio)?

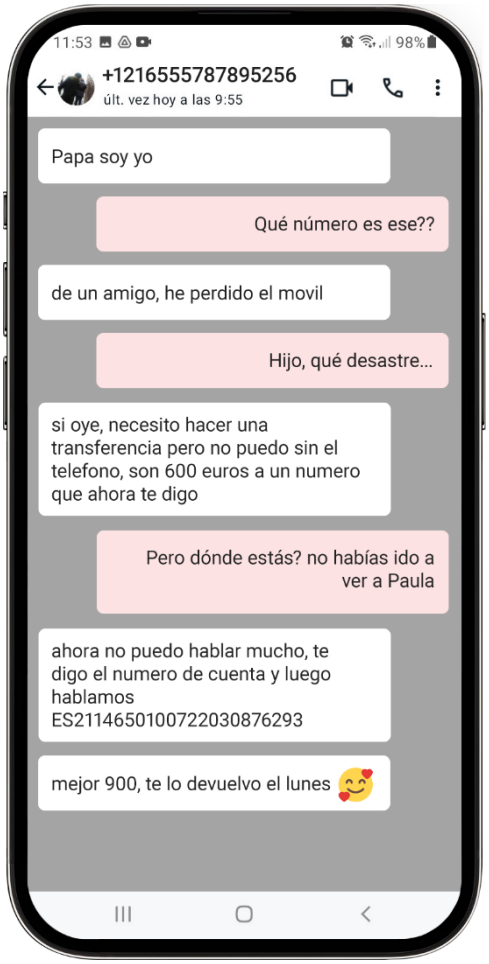
a) Phishing.

b) Smishing.

c) Vishing.

d) No es una estafa.

3. ¿Qué tipo de estafa es esta?



a) Vishing.

b) Smishing.

c) Suplantación de identidad por WhatsApp.

d) No es una estafa.

Ejercicios individuales

- Busca información sobre las cadenas de WhatsApp.
- ¿Qué son? ¿Alguna vez has recibido alguna?
- ¿Qué deberías hacer si te llega una?

3. Caso global para trabajar

Se trata de que, de manera grupal ante un planteamiento, los grupos escojan cómo resolver la situación y posteriormente expliquen el porqué de su elección.

Caso. Investigar el siguiente mensaje de WhatsApp:

Con lo que hemos trabajado a lo largo del taller, hay que determinar si es o no una estafa.

- ¿Es un mensaje verdadero o es una estafa?
  - Respuesta: estafa.
- ¿Por qué? Argumentar la respuesta.
  - Respuesta: mensaje proviniente de un número extraño solicitando dinero urgentemente en nombre de una entidad conocida.
- Reflexionar. ¿Es recomendable compartirlo?
  - Respuesta: No y además es conveniente avisar al entorno.

4. Solucionario

2.1. QUÉ ES LA CIBERSEGURIDAD

1-b, 2-a

2.2. GESTIÓN DE CONTRASEÑAS

1-a, 2-a, 3-b

2.4. NAVEGACIÓN SEGURA

1-b, 2-a, 3-a, 4-b

2.5. IDENTIFICAR ESTAFAS

1-a, 2-c, 3-c

CRÉDITOS

Esta obra ha sido editada y coordinada por Fundación Telefónica.

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