

Programa de formación “Amigabilidad digital”

Taller 1

Seguridad y confianza digital



- 
1. Introducción a la seguridad digital
 2. Gestión de contraseñas y privacidad
 3. Navegación Segura por Internet
 4. Estafas frecuentes y cómo evitarlas
 5. Seguridad en las aplicaciones de mensajería - WhatsApp
 6. Consejos para utilizar tu smartphone manera segura



1. Introducción a la Seguridad Digital



¿Qué es la Seguridad Digital?

Hoy en día, los dispositivos móviles se han convertido en una parte esencial de nuestras vidas.

Con ellos no solo nos comunicamos, sino que también realizamos transacciones bancarias, almacenamos información personal y profesional, y navegamos por internet.

La seguridad digital se refiere a proteger nuestra información personal cuando usamos internet o nuestros dispositivos electrónicos, como teléfonos y ordenadores.

Esto incluye proteger nuestras contraseñas, evitar virus y estar seguros cuando navegamos por la web o usamos aplicaciones. **Es como ponerle una cerradura a nuestras puertas, pero en el mundo digital.**



La Importancia de la Seguridad Digital

La seguridad digital te permite navegar por internet con tranquilidad, sabiendo que estás protegido.

Al usar aplicaciones seguras y evitar las que no lo son, reduces el riesgo de que te roben o hagan daño. También te ayuda a mantener el control sobre tu privacidad, es decir, decidir qué información compartir y con quién.

Así, podrás disfrutar de la tecnología sin preocupaciones ni miedos, y podrás usar internet de manera más libre y segura.



Términos Básicos en Seguridad Digital

Contraseñas: Son claves que protegen el acceso a tus cuentas en línea. Es importante usar contraseñas fuertes y únicas para cada cuenta.

Aplicaciones Seguras: Son programas que provienen de fuentes confiables, como tiendas oficiales (Google Play, App Store). Estas aplicaciones ayudan a proteger tu dispositivo de virus y amenazas.

Navegación Segura: Es el proceso de acceder a sitios web que garantizan una conexión segura, protegiendo tu información personal mientras navegas.



A hand holding a white card with a gold chip, positioned over a laptop keyboard. The background is a blurred laptop keyboard and screen.

2. Gestión de contraseñas y privacidad



¿Qué hace una Contraseña segura?

Longitud: Debe tener al menos 12 caracteres.
Cuanto más larga, más difícil de adivinar.

Combinación: Usa una mezcla de letras (mayúsculas y minúsculas), números y símbolos. Esto aumenta la complejidad y dificulta los intentos de hackeo.

Consejos:

- **Cambia las contraseñas regularmente:**
Actualiza tus contraseñas cada 3-6 meses.
- **No uses la misma para todas tus cuentas:**
Cada cuenta debe tener una contraseña única para minimizar los riesgos.



Cómo recordar y gestionar contraseñas

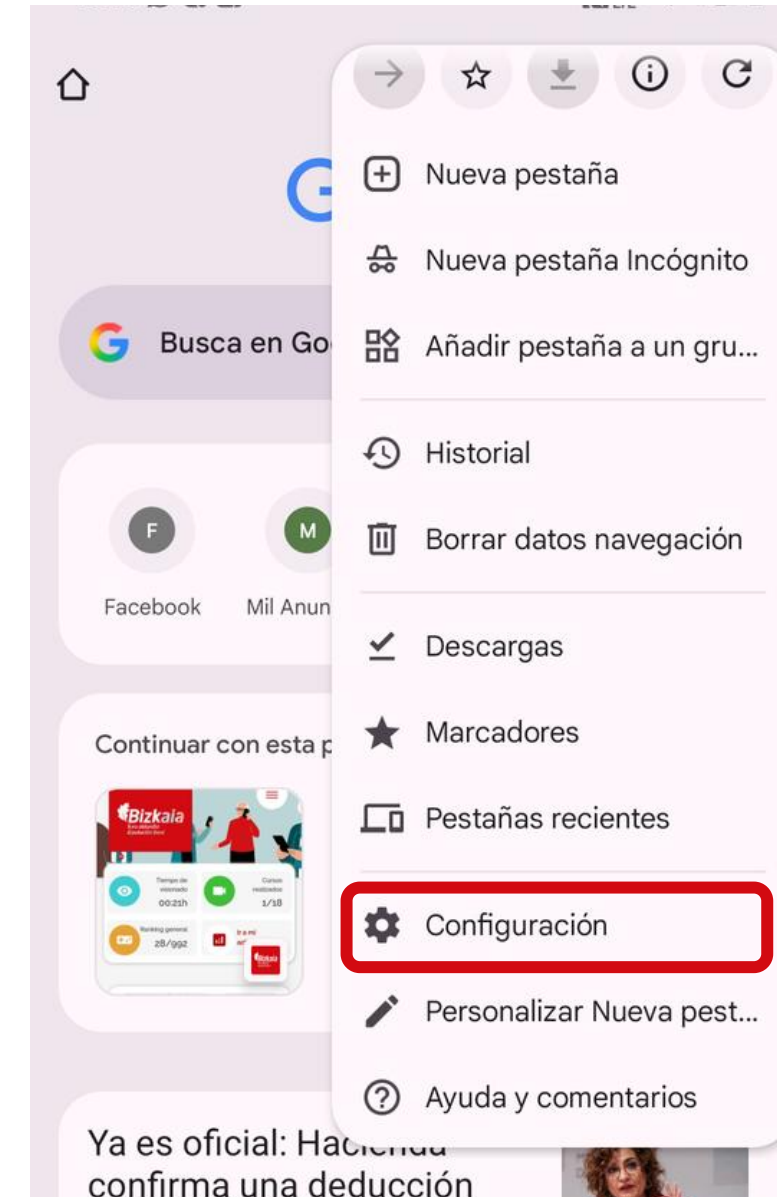
Uso de gestores de contraseñas: Son aplicaciones que guardan todas tus contraseñas de forma segura para que no tengas que memorizarlas. Tú solo recuerdas una contraseña principal y el programa se encarga del resto. Son como una libreta digital con candado.

Frase secreta: En lugar de una palabra, usa una frase fácil de recordar para ti, por ejemplo: "MiPerroSeLlamaToby2020!". Así es más larga, más segura y más sencilla de memorizar.



Gestor de contraseñas

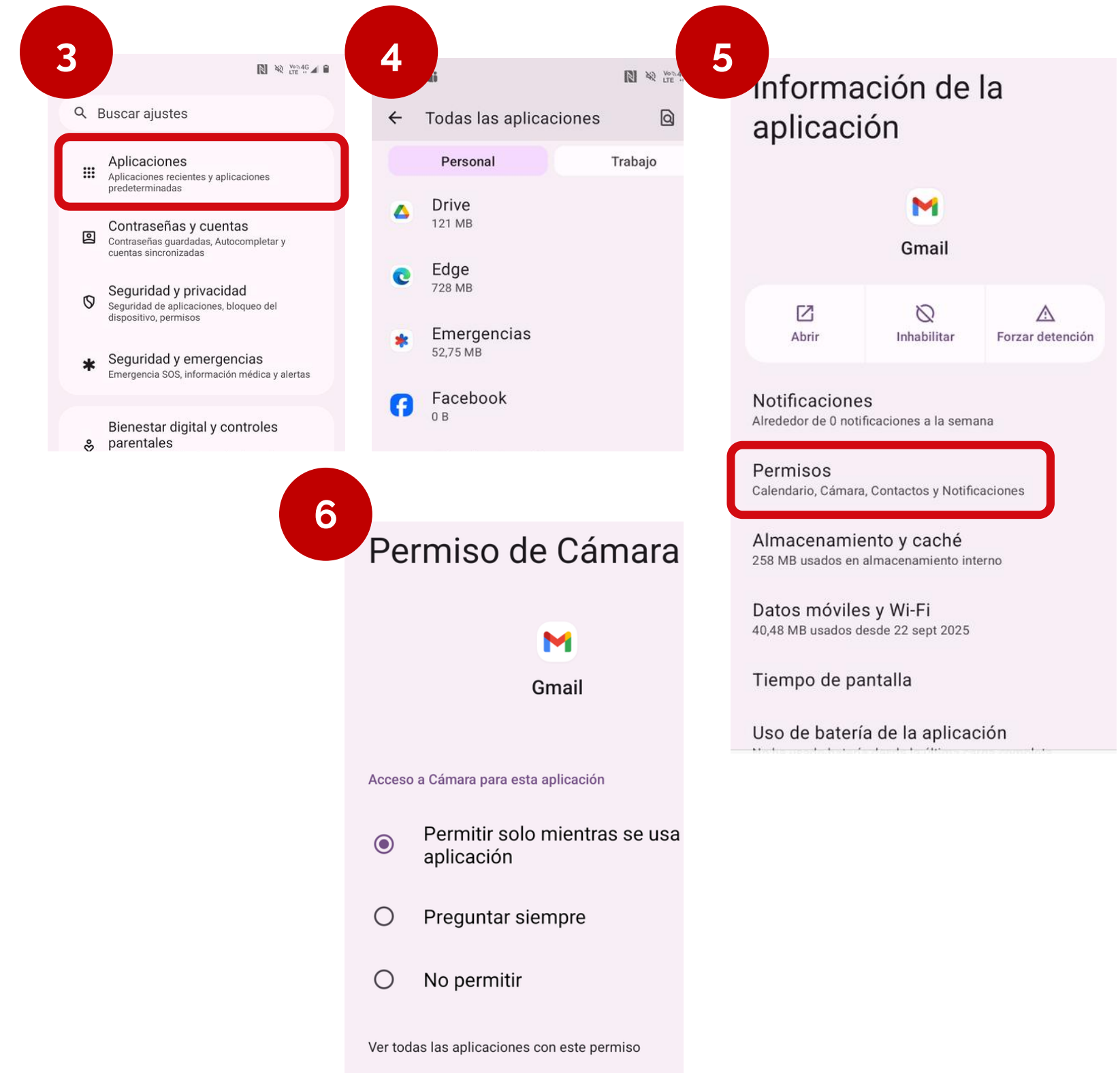
- 1. Abre tu navegador:** Abre Google Chrome o tu navegador preferido.
- 2. Accede al Menú de Configuración:** Haz clic en los tres puntitos en la esquina superior derecha de la pantalla (junto al icono de tu perfil) y selecciona "Configuración".
- 3. Accede al Gestor de Contraseñas:** Aparecerá una opción llamada "Gestor de Contraseñas". Haz clic sobre ella para acceder a todas tus contraseñas guardadas.
- 4. Gestiona tus contraseñas:** Aquí podrás ver todas las contraseñas guardadas en tu cuenta de Google. Puedes buscar, ver o eliminar contraseñas, o agregar nuevas.



Privacidad: Ver y ajustar los permisos de las Apps

Ajustar permisos de una aplicación específica:

1. Abre la Configuración de tu dispositivo Android.
2. Desplázate hacia abajo y selecciona Aplicaciones o Aplicaciones y notificaciones (dependiendo de tu versión de Android).
3. Toca Ver todas las aplicaciones o Aplicaciones instaladas.
4. Selecciona la aplicación de la que deseas ver los permisos.
5. En la página de la aplicación, toca Permisos.
6. Aquí podrás ver y modificar los permisos de la aplicación (por ejemplo, acceso a la cámara, micrófono, ubicación, contactos, etc.). Puedes activar o desactivar los permisos según lo que consideres necesario.

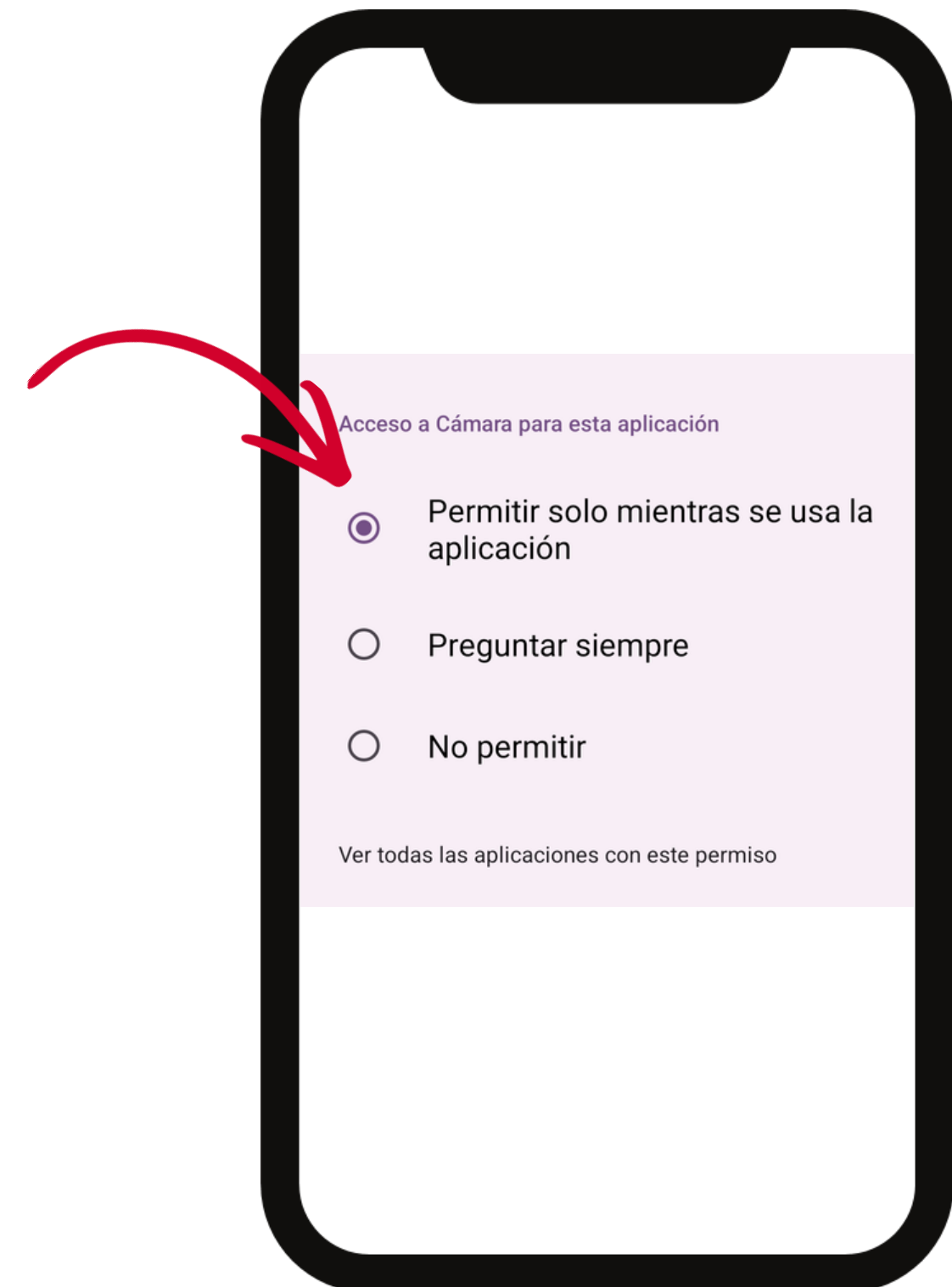


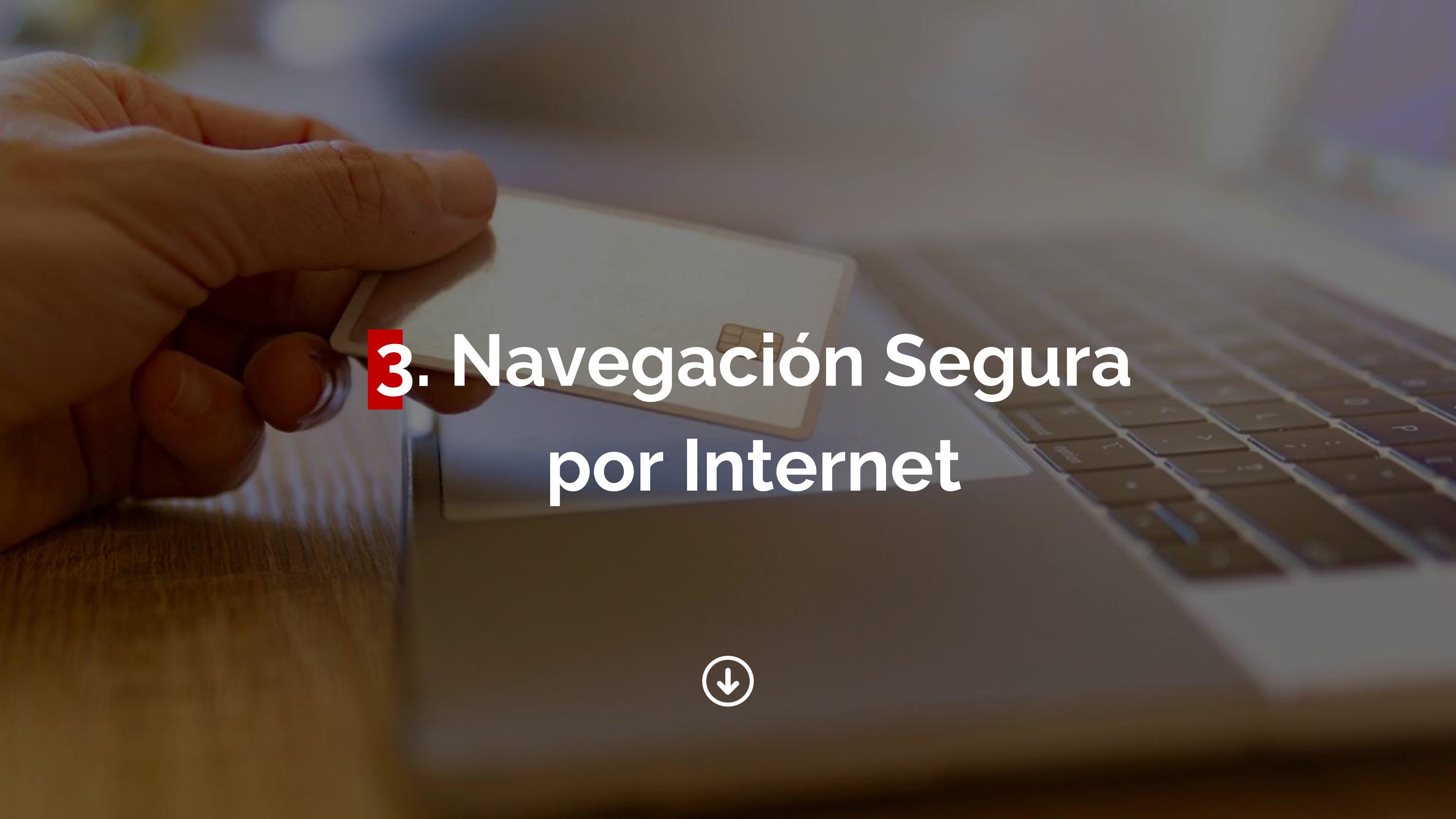
Privacidad: Consejos para ajustar los permisos de las Apps

Desactivar permisos no esenciales: Revisa y desactiva permisos que no sean necesarios, como el acceso a contactos en una aplicación de linterna.

Revisar acceso a ubicación: Desactiva el permiso de ubicación para aplicaciones que no necesiten acceder a tu localización.

Controlar permisos de aplicaciones instaladas: Ajusta los permisos de acceso a contactos, almacenamiento y otros datos sensibles directamente desde la pantalla de permisos de la aplicación.



A hand is holding a silver credit card over a laptop keyboard. The background is a blurred laptop screen and keyboard. The text '3. Navegación Segura por Internet' is overlaid on the image.

3. Navegación Segura por Internet



Cómo navegar de forma segura

1. Reconocer Sitios Seguros: Busca "https://": La "s" al final de "http" significa que el sitio web tiene cifrado SSL, lo que protege tu información al navegar.

2. El candado en la barra de direcciones: Al lado de la URL, el ícono de candado indica que la conexión es segura. Asegúrate de que siempre aparezca antes de ingresar información personal o financiera.

3. Desconfía de sitios sin "https" o sin el candado: Si el sitio no tiene estos indicativos de seguridad, es mejor no interactuar con él, especialmente si vas a introducir información sensible como contraseñas o datos bancarios.



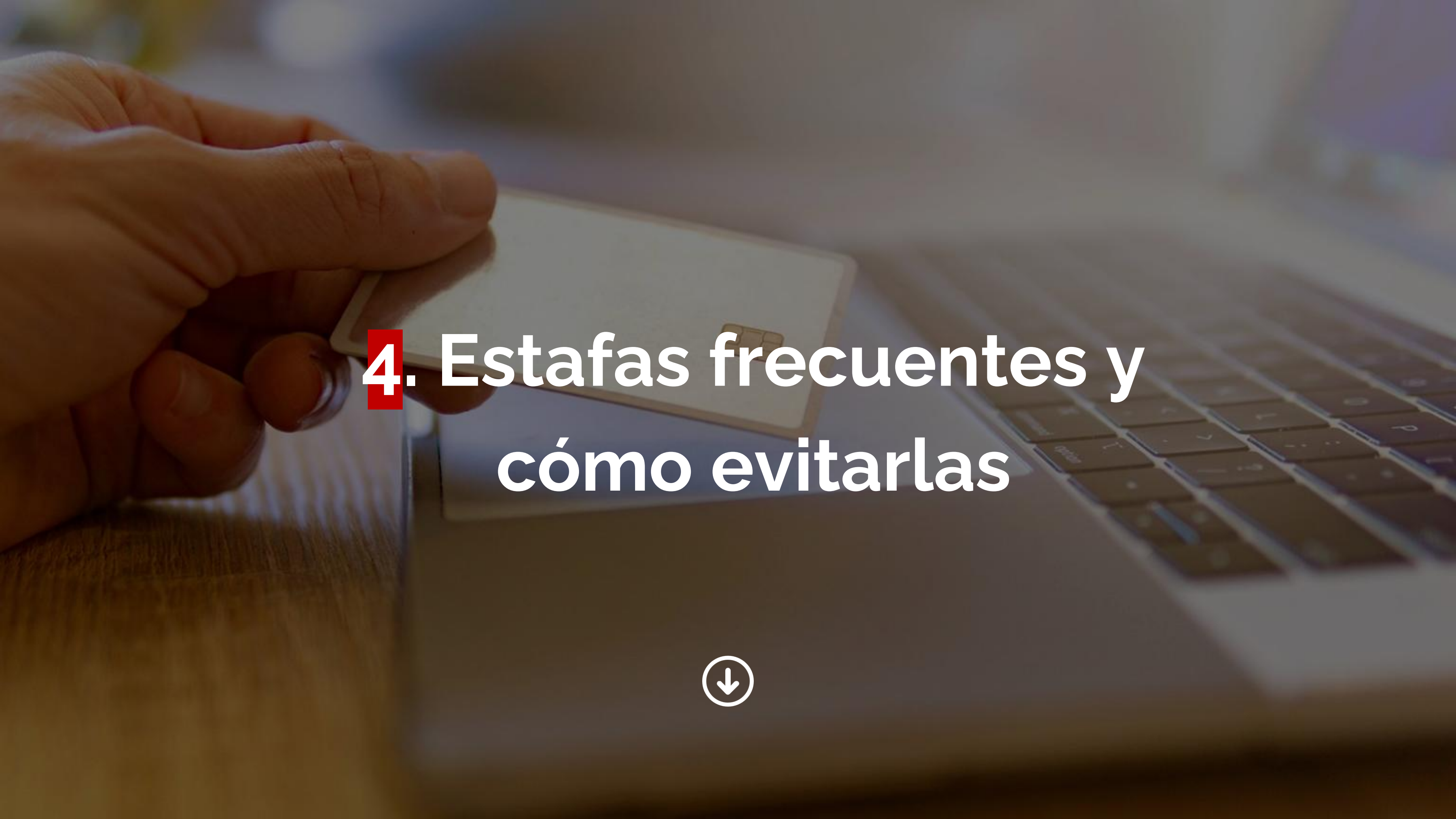
Redes Wi-Fi públicas sí, pero con cautela

Podemos utilizar una red Wi-Fi pública, por ejemplo, en un restaurante o cafetería, para navegar y consultar alguna página web.

Pero estas redes no son las más recomendables para acceder, por ejemplo, a nuestro banco o realizar compras online donde debemos introducir datos personales, bancarios o contraseñas.

Por lo tanto, al utilizar redes Wi-Fi públicas debemos tener siempre la precaución de no introducir datos personales, aunque estemos en las páginas oficiales.



A hand is holding a light-colored credit card over a laptop keyboard. The background is blurred, showing the laptop and a wooden surface.

4. Estafas frecuentes y cómo evitarlas



Evitar estafas de Phishing en Internet

¿Qué es el Phishing?

El phishing es un engaño en el que una persona malintencionada se hace pasar por alguien de confianza (como un banco, una tienda o un amigo) para robar tu información personal.

Normalmente, el phishing ocurre a través de correos electrónicos, mensajes de texto o redes sociales que contienen enlaces falsos.

Si haces clic en estos enlaces, podrías ser redirigido a una página falsa que intenta obtener tus datos, como tu contraseña, número de tarjeta bancaria o dirección.

Felicitaciones a nuestros 3 clientes de Media Markt que ganaron: 1 Manuel 2 Ana 3 Inma
Confirme aquí:
<https://protectlnk.com/T693TkW>.

1 14:37

mié 29 de ene 15:20

Rappi: ¡Tienes un regalo! 45 Rappicredits para que comas en los mejores restaurantes
<https://rappi.app.link/Ein6PQnEu3> hasta las 6 PM.
T&C

Actualización de datos personales

ING
People in progress

Hola,

En ING queremos estar cerca de ti y poder ofrecerte un servicio cada día mejor.

Para ello, es necesario que actualices tus datos personales entrando en el "Área Clientes" de nuestra web y siguiendo los pasos que te indicaremos.

[Área Clientes](#)

Atentamente,

ING

IMPORTANTE: No contestes a este correo, la dirección desde la que se envía este mensaje no está habilitada para la recepción de mensajes. Recuerda que ING nunca te enviará por correo electrónico solicitud alguna para que informes de tus datos personales ni de tus claves.

¿Cómo podemos identificar estos fraudes?

Para identificar estos mensajes fraudulentos nos fijaremos en los siguientes puntos:

1. Remitente: Si nos fijamos en el remitente, sus datos nos parecerán extraños. En el ejemplo, nos escribe una dirección de correo desconocida.
2. Logos de las marcas: Los logos suelen estar desnivelados, no acordes con el mensaje. Se ven peor y son de mala calidad, poco profesionales.
3. Contenido y redacción: Normalmente está desordenado, desestructurado, con faltas gramaticales y de ortografía. Es raro.
4. Enlaces e información: Incorporan un link que no sabemos dónde nos lleva y nos piden datos personales, cuentas o claves privadas.

1

De: Banco santander <Refd-ancomal@ovpn.se>

Enviado: lunes, 3 de junio de 2019 7:29

Para:

Asunto: Recordatorio final: el estado de la cuenta ha sido modificado

2



3

Buenos Dias !

Asunto : Error de sesion

Remitente : Servicio al cliente.

Lamentamos informarle que su ultima sesión al servicio santander en linea no finalizo de manera correcta.

así que por su seguridad le pedimos termine la sesión de inmediato.

Para evitar que su acceso sea manejado por personas ajenas a usted :

4

[Haga clic aqui,y iniciar sesion en su cuenta](#)

Este es un mensaje automático. Por favor no les contestes Gracias por confiar en nosotros.

Equipo de Atención al Cliente.santander ,

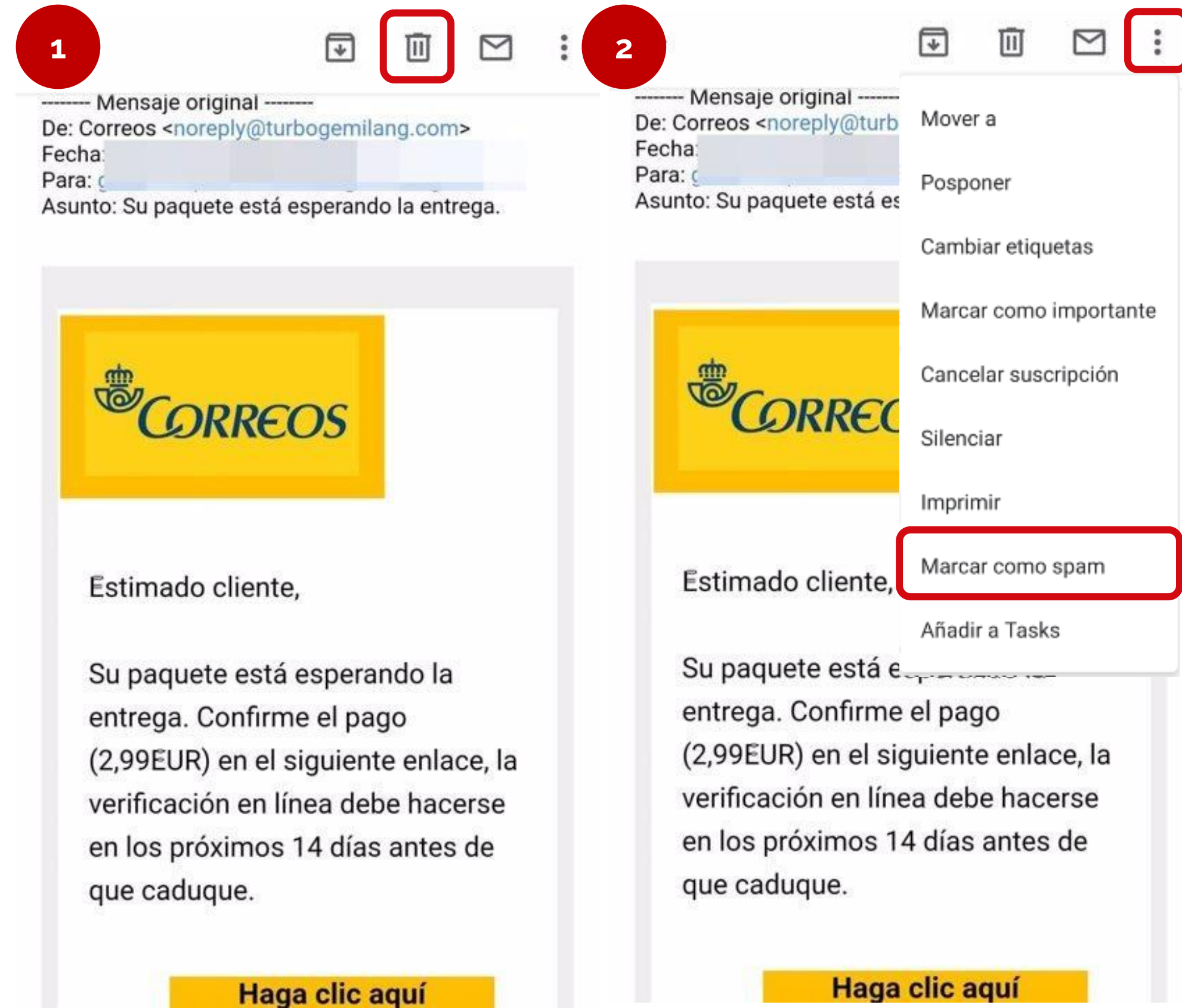
santander es una marca registrada. Todos los derechos reservado

¿Cómo actuamos ante estos mensajes?

Lo primero y por supuesto:

1. **No responder:** No responderemos al mensaje, SMS o email.
2. **No pinchar en el link:** No pincharemos en los links sospechosos que incorporan.
3. **No dar ningún dato:** En ningún caso daremos ninguno de los datos que nos solicitan.
4. **Borrar mensaje y bloquear/marcar como spam:** En ningún caso daremos ninguno de los datos que nos solicitan.

Recuerda: En ningún caso debemos proporcionar ninguno de los datos que nos solicitan. Siempre mantén tu información personal segura.



¿Qué hacer si caíste en una estafa de Phishing?

- **Cambia tus contraseñas inmediatamente:**
Si crees que compartiste información sensible, cambia las contraseñas de tus cuentas en línea.
- **Avísales a las instituciones afectadas:**
Si diste tu número de tarjeta o datos bancarios, contacta a tu banco para bloquear la tarjeta o cuenta.
- **Reporta la estafa:**
Puedes reportar el phishing a tu proveedor de correo electrónico o a las autoridades para ayudar a prevenir futuros fraudes.



A hand is holding a white SIM card over a laptop keyboard. The background is a blurred image of a laptop and a desk.

5. Seguridad en las aplicaciones de mensajería - WhatsApp



Mantener conversaciones seguras

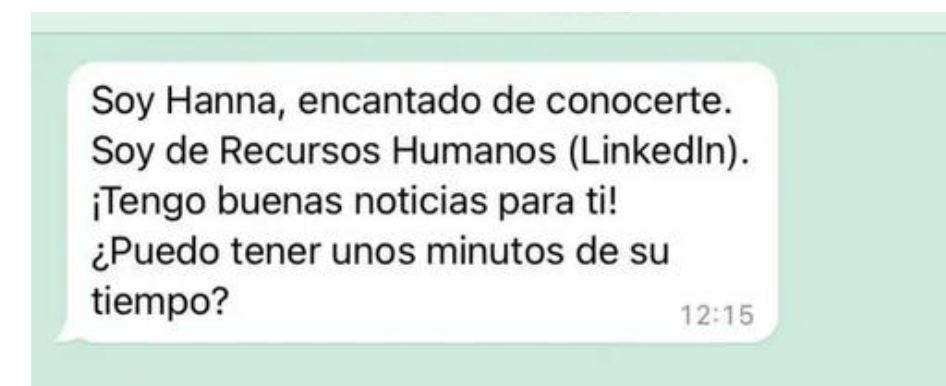
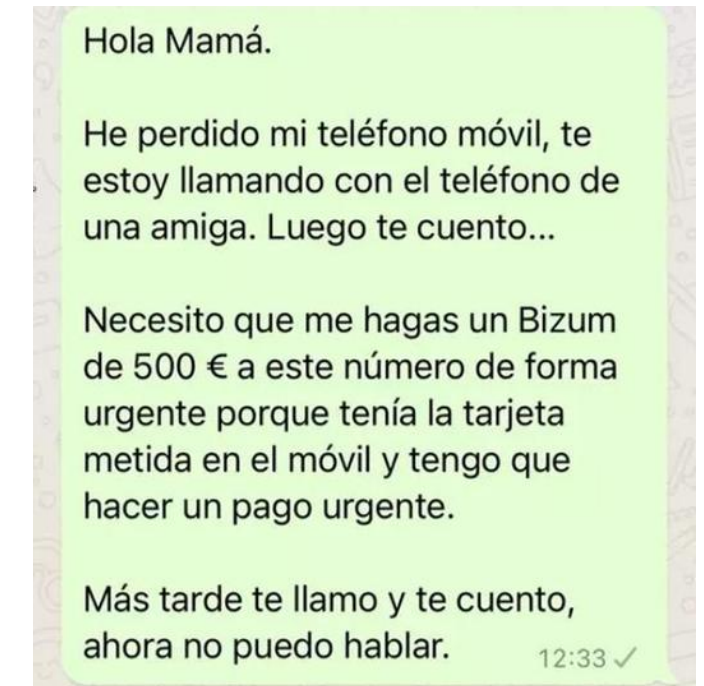
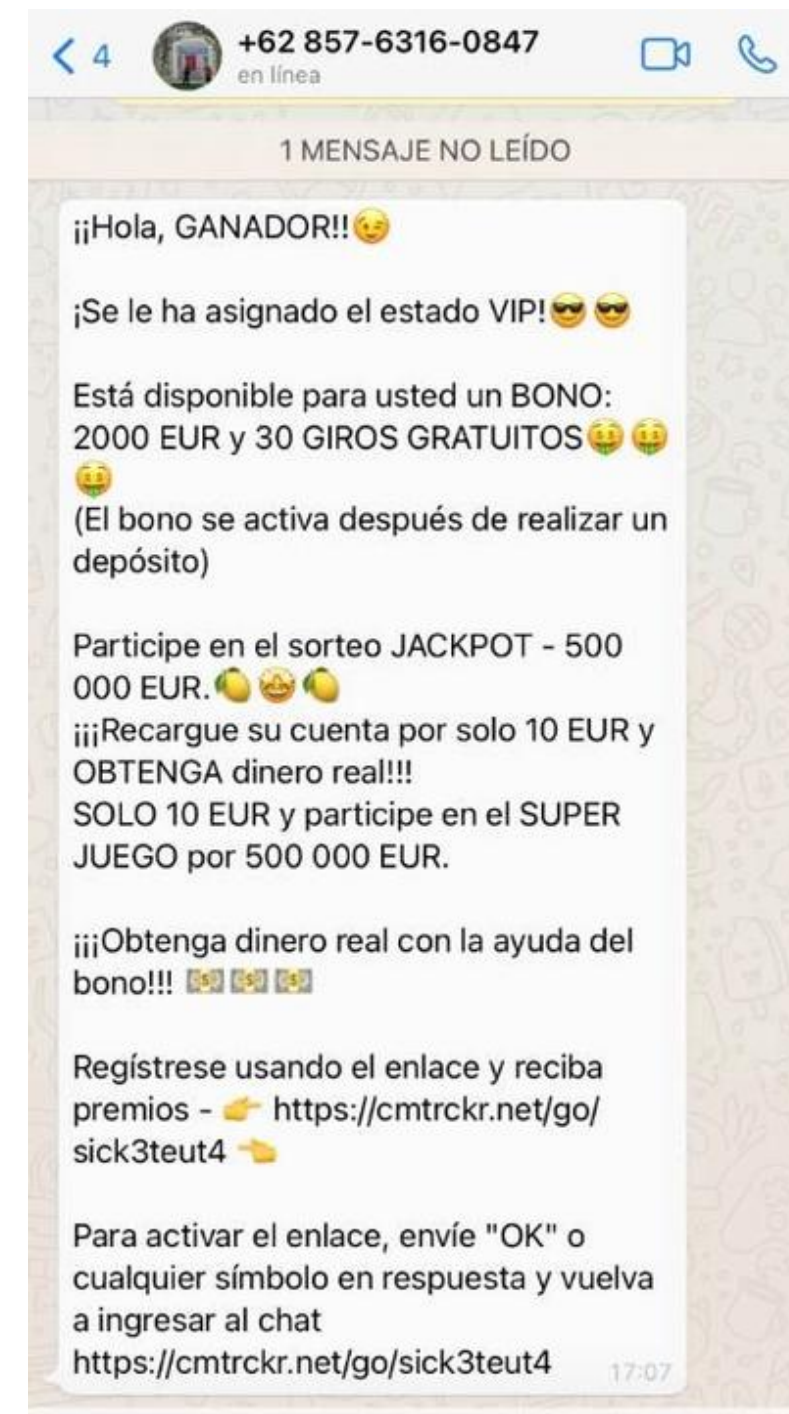
- 1. Evita enviar datos personales:** No responderemos al mensaje, SMS o email.
- 2. No hagas transacciones financieras a través de mensajes:** No pincharemos en los links sospechosos que incorporan.
- 3. Cuidado con los mensajes de extraños:** Si recibes mensajes de desconocidos pidiéndote información personal, no respondas. Muchas veces, esto es un intento de fraude.
- 4. Evita hablar de salud y situaciones personales:** No discutas detalles de tu salud, ubicación exacta, ni situaciones familiares delicadas por aplicaciones de mensajería. Los delincuentes pueden usar esa información en tu contra.



Estafas comunes en WhatsApp

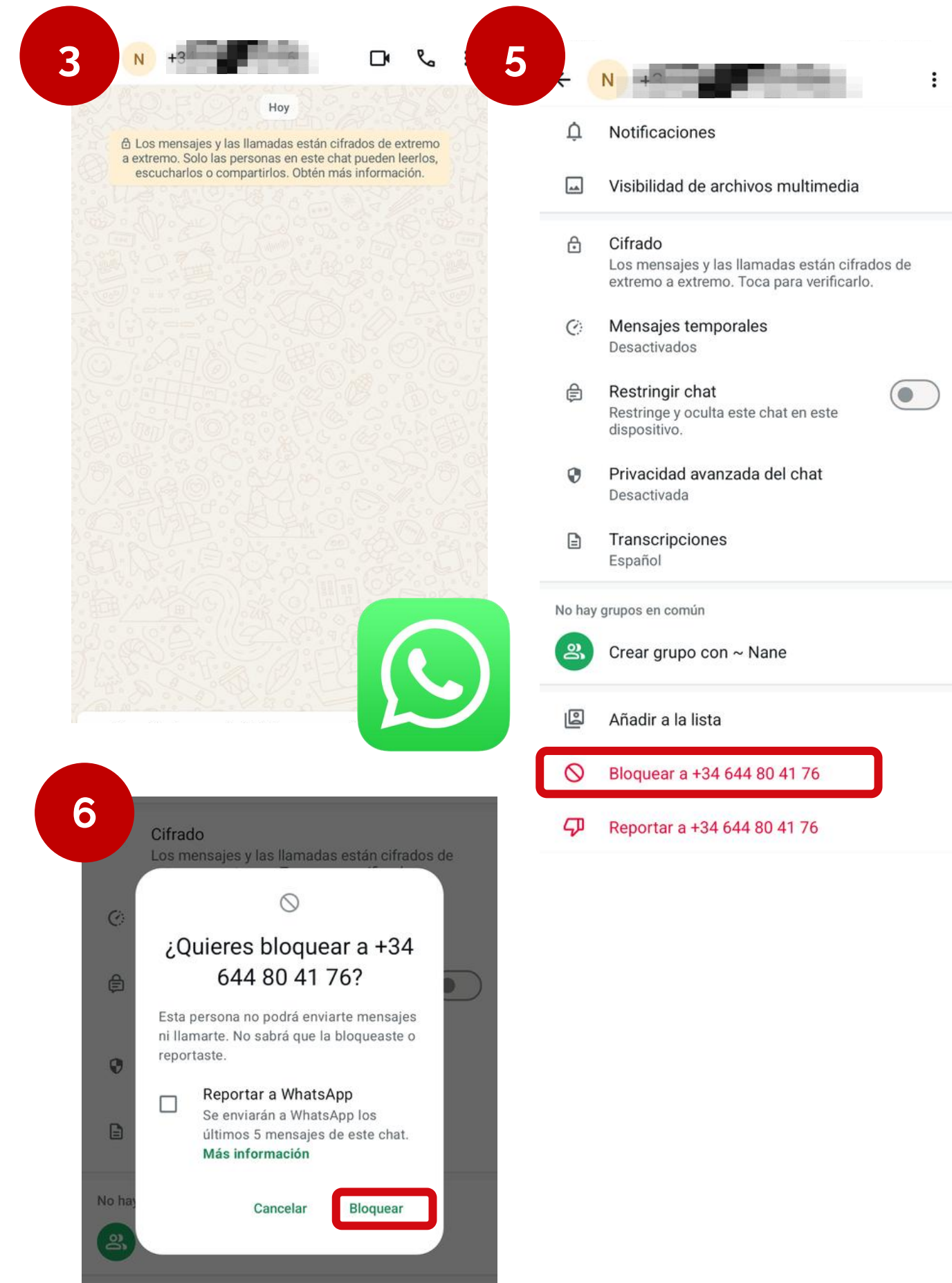
WhatsApp puede ser un lugar donde ocurren estafas, por eso es importante reconocer los mensajes sospechosos para proteger nuestra información personal y evitar ser engañados.

- **Falsos premios o sorteos:** Si crees que compartiste información sensible, cambia las contraseñas de tus cuentas en línea.
- **Estafas de "Amigos en apuros":** Un mensaje de un "amigo" o familiar pidiendo dinero urgente, pero en realidad es un estafador.
- **Falsos enlaces o actualizaciones:** Te envían un enlace que parece oficial para "actualizar" WhatsApp, pero al hacer clic, tu información personal puede ser robada.
- **Ofertas falsas de trabajo o inversiones:** Recibes mensajes de trabajos fáciles o inversiones que prometen ganar mucho dinero, pero todo es falso.



Cómo bloquear en WhatsApp

- 1. Abre WhatsApp:** Toca el ícono de WhatsApp en tu teléfono para abrir la aplicación.
- 2. Ve a la conversación:** Si la persona extraña te ha enviado un mensaje, abre la conversación con esa persona.
- 3. Toca el número/nombre de la persona:** En la parte superior de la pantalla, verás el nombre o número de teléfono de la persona. Tócalo para abrir los detalles de la conversación.
- 4. Desplázate hacia abajo:** Baja hasta el final de la pantalla de información de la persona.
- 5. Toca "Bloquear contacto":** Verás la opción "Bloquear contacto". Tócala.
- 6. Confirma el bloqueo:** Aparecerá una ventana pidiéndote que confirmes si deseas bloquear a la persona. Toca "Bloquear" para confirmar.



A hand is holding a white SIM card over a laptop keyboard. The background is a blurred laptop screen and keyboard. The text is overlaid on the image.

6. Consejos para utilizar tu smartphone manera segura

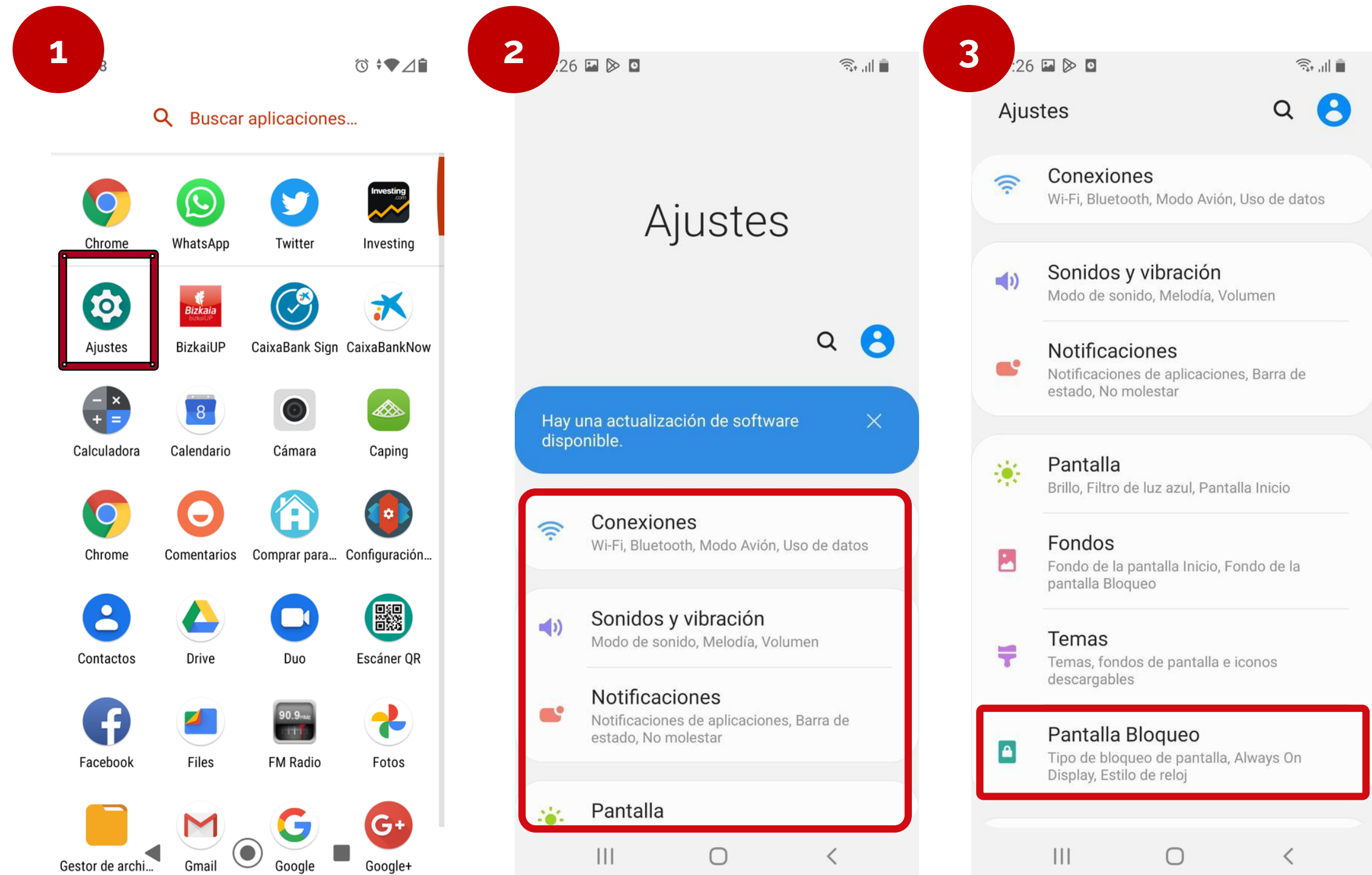


Código o patrón de desbloqueo (I)

Si nos robasen el móvil, nos gustaría que no pudieran desbloquearlo y acceder a su contenido. Para ello, podemos establecer un código o patrón de desbloqueo, de manera que quien no lo sepa no pueda desbloquear el móvil ni acceder a él.

Veamos cómo se hace y las opciones que tenemos.

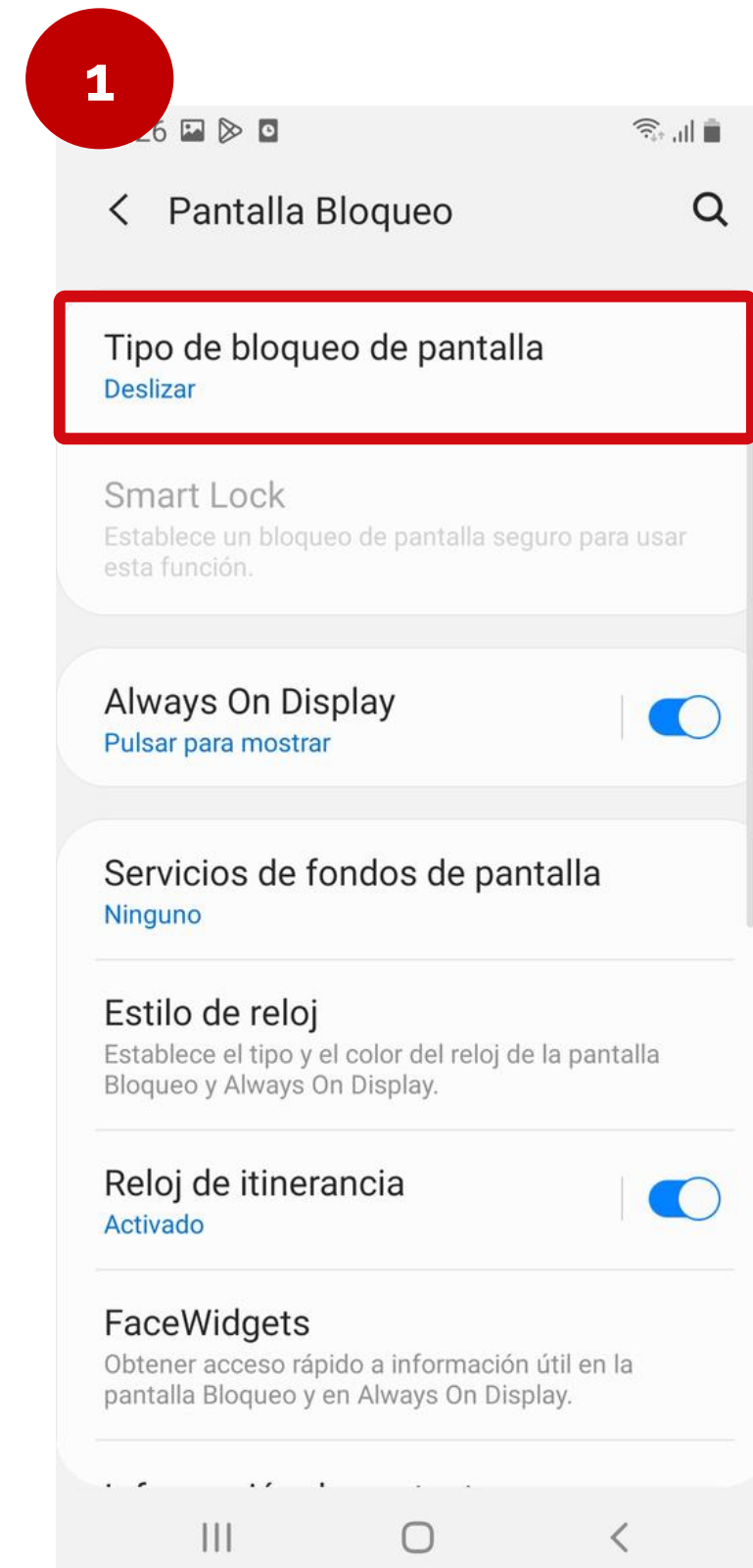
1. Clicaremos encima del icono "Ajustes".
2. Una vez dentro, se nos desplegarán diferentes opciones.
3. Buscaremos y clicaremos encima de "Pantalla Bloqueo".



Código o patrón de desbloqueo (II)

4. Dentro de “Pantalla Bloqueo”, clicaremos en “Tipo de bloqueo de pantalla” donde podremos seleccionar el tipo de bloqueo que queremos.
5. En “Tipo de bloqueo de pantalla” veremos las opciones a nuestra disposición:
 - **Deslizar:** Se desbloqueará deslizando nuestro dedo, opción poco segura y no recomendable.
 - **Patrón:** Nos permitirá crear un patrón de desbloqueo, opción recomendable.
 - **PIN:** Nos solicitará el código PIN para desbloquearlo.
 - **Contraseña:** Nos permitirá crear una contraseña para desbloquearlo.
 - **Ninguno:** No tendremos bloqueada la pantalla, opción poco segura y no recomendable.

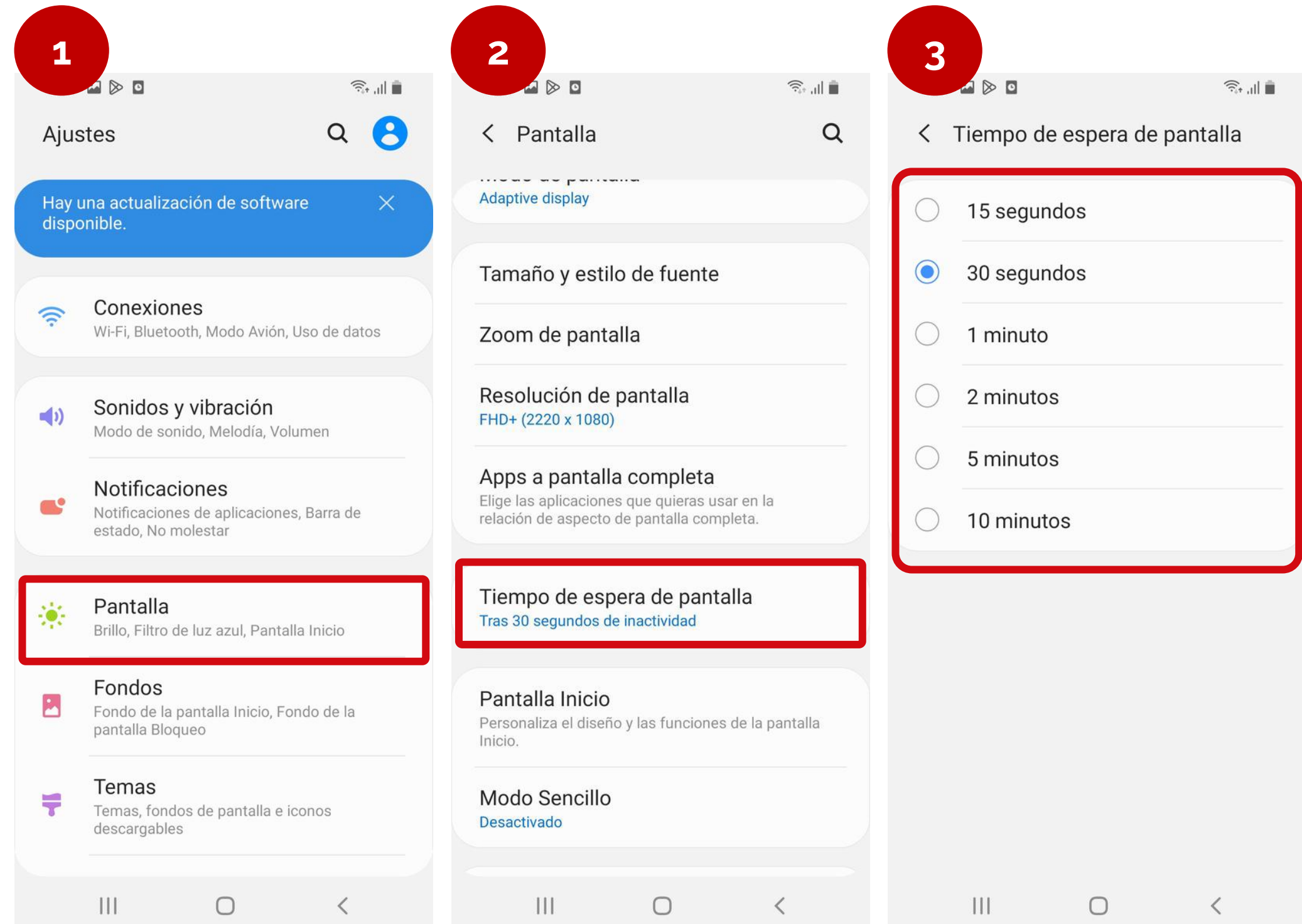
Para establecer el sistema de bloqueo, seleccionaremos una de las tres opciones recomendadas (Patrón, PIN, Contraseña), y seguiremos las instrucciones para configurarlo.



Tiempo de bloqueo automático de la pantalla

Es importante que disminuyamos el tiempo que tarda en bloquearse la pantalla del teléfono cuando no lo estamos utilizando. Para configurarlo:

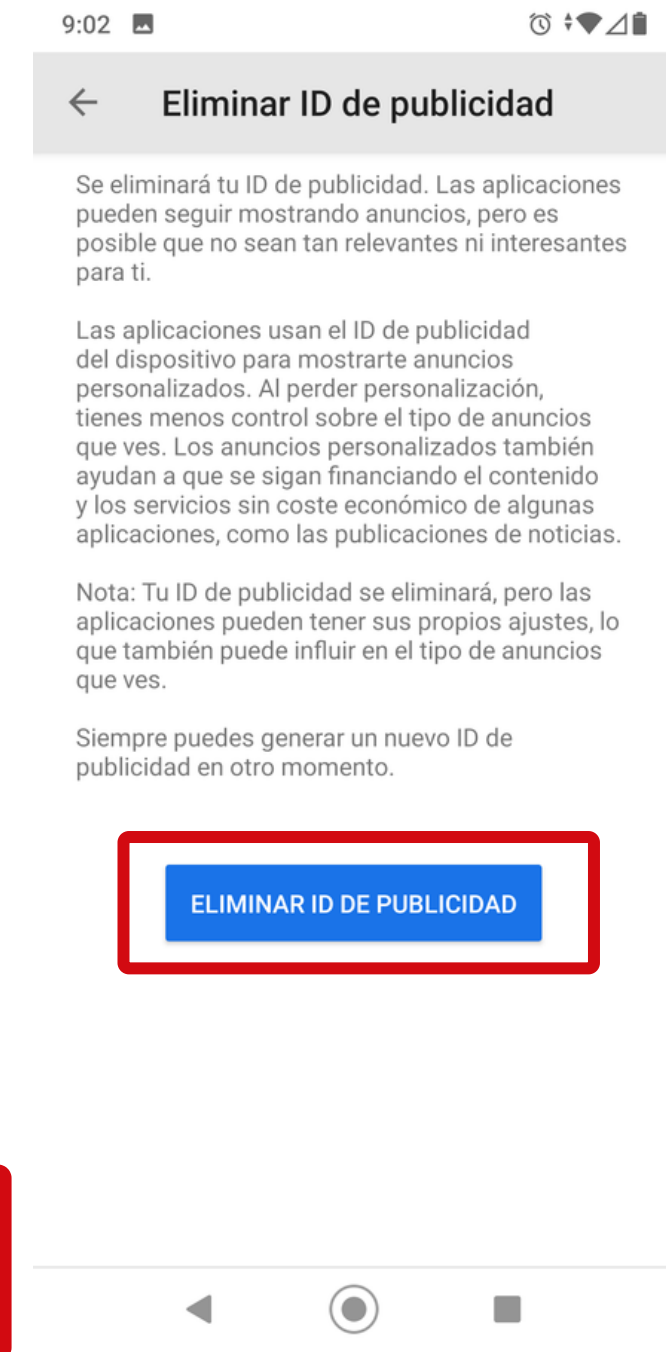
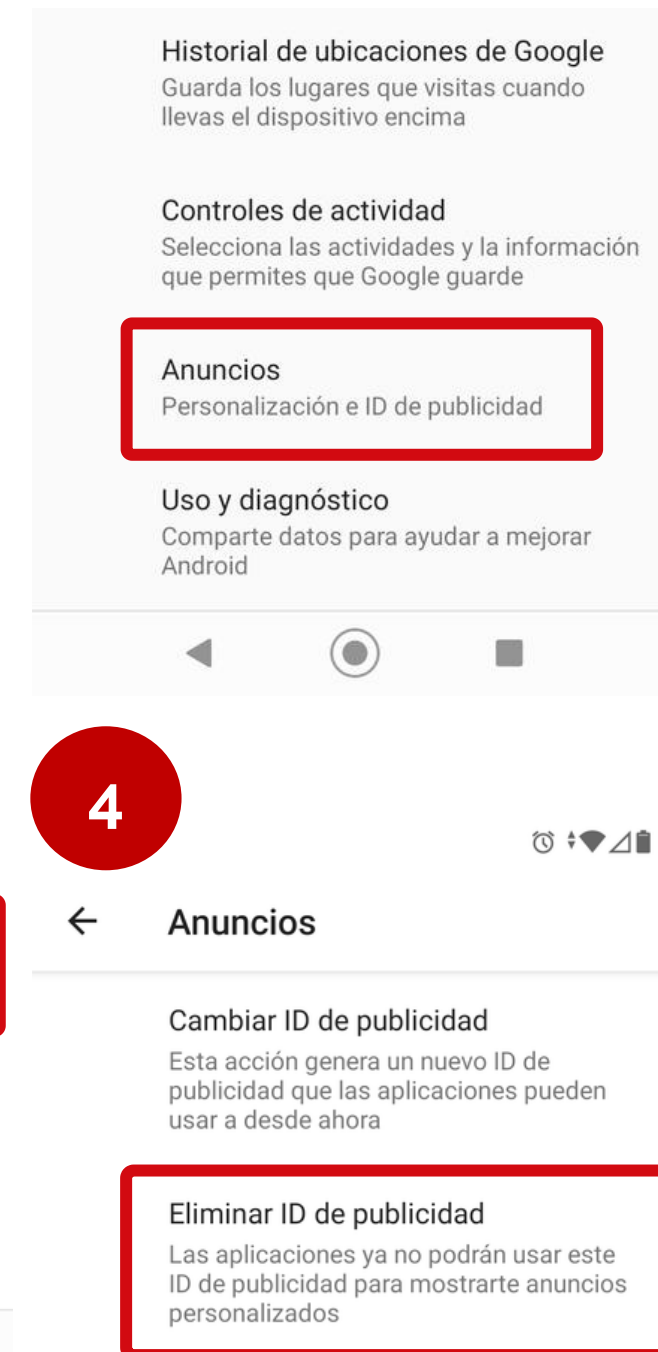
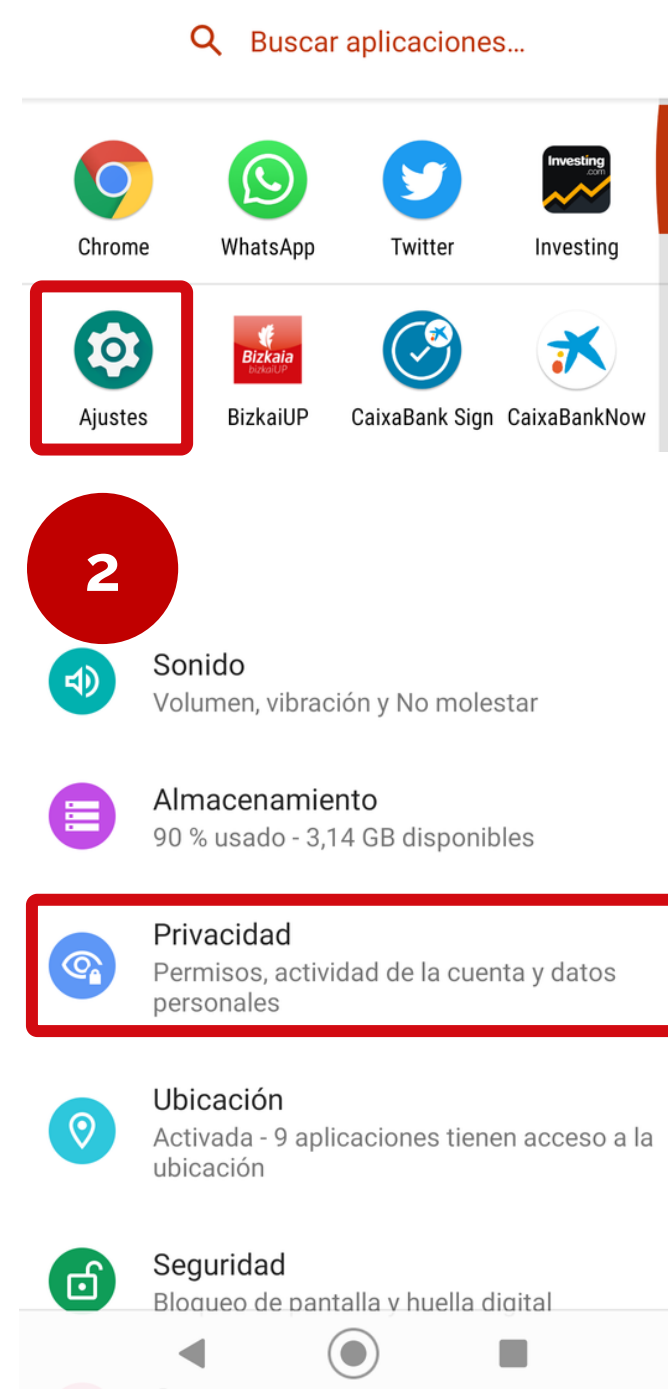
1. Accederemos a **“Ajustes”** y después clicaremos la opción “Pantalla”.
2. Buscaremos la **opción “Tiempo de espera de pantalla”** y clicaremos en ella.
3. Se desplegarán las diferentes opciones disponibles de tiempo de espera de pantalla. **No es recomendable que este tiempo sea superior a 30 segundos.** De este modo si no estamos usando el móvil y pasan más de 30 segundos, se bloqueará la pantalla y deberemos introducir el patrón de desbloqueo para volver a acceder al móvil.



Evitar anuncios en base a búsquedas realizadas

Es muy común que busquemos algún término en internet o naveguemos por una página web, y que después nos aparezcan anuncios y publicidad en otras páginas web sobre lo que hemos estado buscando. Podemos configurar nuestro smartphone para no padecer esta situación.

1. Entraremos en los **“Ajustes”** del móvil.
2. Buscaremos y clicaremos después en **“Privacidad”**.
3. Después, clicaremos en la opción **“Anuncios”**.
4. Después, clicaremos en la opción **“eliminar ID de publicidad”**.
5. En la última pantalla clicamos en el botón **“Eliminar ID de publicidad”**. De este modo, nuestro teléfono no nos mostrará anuncios basados en nuestros términos de búsqueda o histórico de páginas web visitadas.





Adiskidetz​a Digitala

Amigabilidad Digital