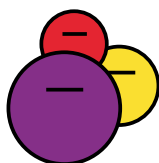
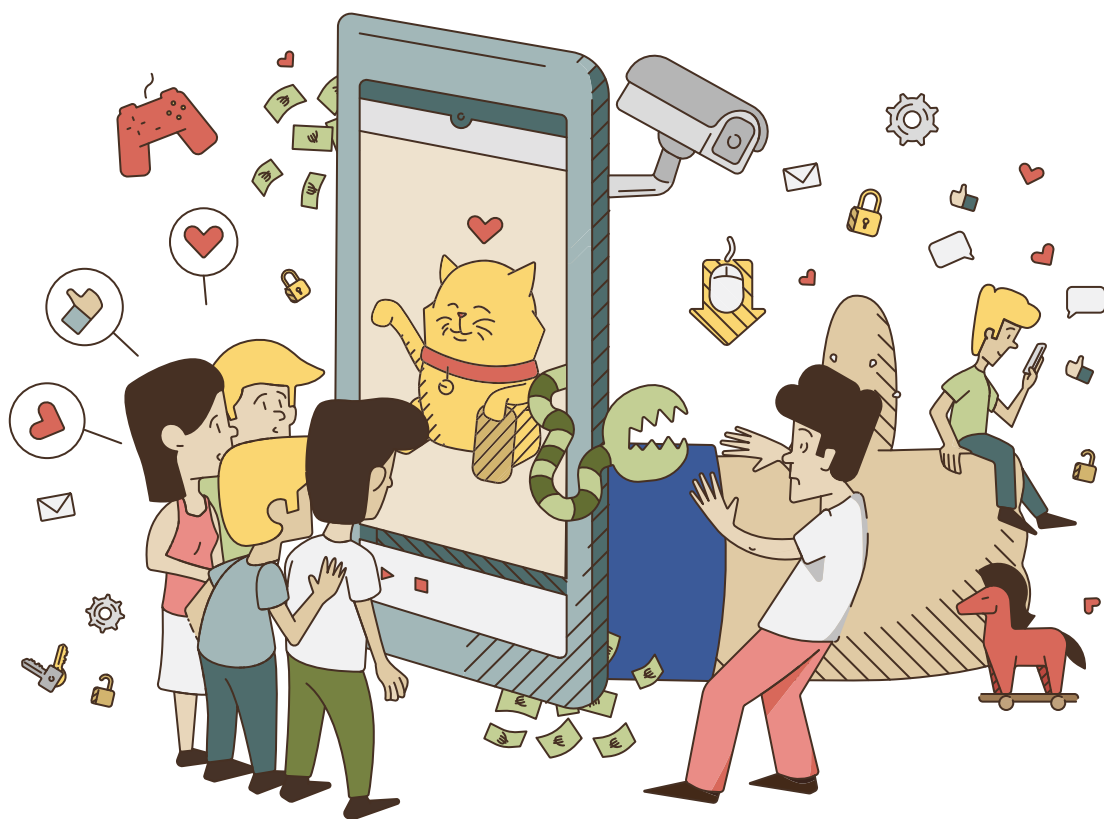


Los 10 principales retos que debes
enfrentar en el entorno digital

GUÍA PARA EL USO
**RESPONSABLE Y SEGURO DE
INTERNET**



ADICAE

Asociación de Usuarios de,
Bancos, Cajas y Seguros

Presentación

La Asociación de Usuarios, Cajas y Seguros (ADICAE) surge en Zaragoza en 1988 como una organización especializada en la protección, formación, reclamación, información y reivindicación de los derechos de los usuarios de servicios bancarios y seguros. Se ha consolidado como una de las asociaciones de consumidores con mayor presencia en territorio nacional gracias a sus acciones y demandas colectivas a favor de los consumidores, además de por su adaptación a los nuevos medios online.

Desde hace años venimos adaptándonos a la llamada “era digital”. Los hábitos de los consumidores y la economía se han ido transformado a un ritmo vertiginoso, convirtiendo el mundo digital en el eje de casi todas nuestras relaciones. Actualmente, más de 4.300 millones de personas disponen de conexión a Internet. De la misma manera, más de 3.500 millones de individuos se consideran usuarios de redes sociales y las ventas de smartphones siguen creciendo a un gran ritmo en todo el mundo. Estas cifras reflejan, de manera clara, una nueva realidad a la que debemos adaptarnos.

Es por ello, por lo que, desde ADICAE, queremos ser un referente para los consumidores en materia de medios digitales; tales como redes sociales, aplicaciones o plataformas de comercio electrónico, debido a las claras conexiones existentes entre los servicios financieros y el entorno digital que afectan al conjunto de los usuarios.

Por ello, mediante esta guía, hemos querido dotar a los consumidores con las herramientas y nociones necesarias para navegar de forma segura por los entornos digitales. Definir y afrontar los retos que nos propone Internet es la finalidad de esta guía, la cual hemos tratado de hacer lo más fácil y comprensible posible gracias a unas ilustraciones que identifican estos desafíos de una manera visual, rápida y fácil.

En ADICAE estamos convencidos de que los consumidores, como colectivo, tenemos la capacidad de promover un consumo crítico, responsable y solidario de los medios online.

Esperamos que la lectura de esta guía os ayude a descubrir nuevos retos de la era digital y a disfrutar de manera totalmente segura a la hora de navegar e interactuar con las distintas herramientas y dispositivos digitales.

Manuel Pardos

Presidente de ADICAE

Índice

01

Ciberactivismo

El ciberactivismo es un fenómeno referido a la forma de acción política y participación social valiéndose de las ventajas de las nuevas tecnologías.

02

Ventanas emergentes

Son ventanas que emergen automáticamente, sin que el usuario lo solicite, para mostrar publicidad de un modo intrusivo.

03

Phishing

Haciéndose pasar por un sitio de confianza, engaña al usuario para robarle información confidencial.

04

SEM

Es el pago por publicidad en Internet, donde pone en las principales posiciones anuncios que pueden parecer lo más relevante pero realmente no lo son.

05

Protección de datos en RRSS

RRSS son cultivo para el tráfico de datos e información que, probablemente, no querriamos que se divulgue.

06

Influencers ¿Recomendación espontánea o pagada?

La publicidad recurre a caras conocidas y los influencers no son una excepción, pero, la publicidad que realizan, raramente la señalan como tal.

07

Engaños en Internet

En internet hay miles de estafadores que pretenden ganar dinero y obtener datos personales.

08

Privacidad y móviles

Llevamos toda clase de información en nuestros dispositivos móviles, por lo que es fundamental evitar poner en riesgo la integridad de nuestros datos.

09

Nada es gratis

Aplicaciones, RRSS o juegos aparentemente gratis, no lo son ya que si no se cobra por su uso, se cobrará en forma de consumo publicitario o con tus datos personales.

10

Geolocalización invasiva

Actualmente nos geolocalizan por distintos métodos y nos envían notificaciones cuando nos encontramos cerca de comercios para manipularles e incitarles a que entren a sus locales.

CIBERACTIVISMO

El ciberactivismo es un fenómeno referido a la forma de acción política y participación social valiéndose de las nuevas tecnologías, aprovechándose de sus ventajas, como la inmediatez, la viralidad y la horizontalidad de los medios digitales.

VIAS DE MOVILIZACIÓN



Redes sociales



Emails



Aplicaciones de mensajería



VENTAJAS DEL CIBERACTIVISMO



Poder contactar con cualquier parte del mundo.



La posibilidad de difundir masivamente las propuestas de movilización de los consumidores.



La inmediatez de los contactos.



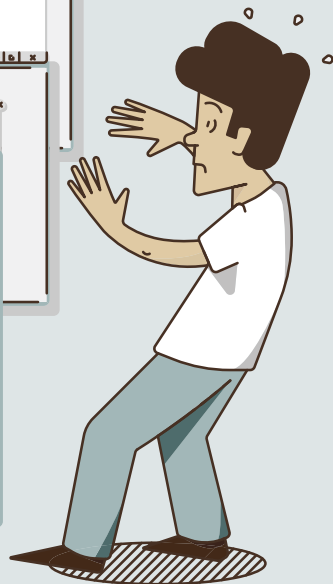
Viralización. Por ejemplo, tras compartirlo con conocidos, estos podrán difundirlo a sus conocidos y así sucesivamente.



Es una herramienta de presión social.

VENTANAS EMERGENTES

Son ventanas que emergen automáticamente, sin que el usuario lo solicite, para mostrar publicidad de un modo intrusivo.

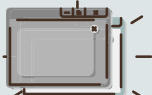


TIPOS DE VENTANAS EMERGENTES



POP-UP

Se superpone a la ventana del navegador que el usuario está observando, tapando el contenido.



POP-UNDER

Se abre una nueva ventana que se sitúa detrás de la ventana que el usuario está observando.



LIGHT BOX

Es un *pop-up* con la particularidad de que oscurece el fondo detrás de él.

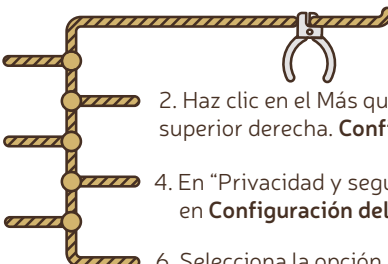


BUCLE DE POP-UPS

Los *pop-ups* activan nuevas ventanas emergentes, creando un bucle casi infinito.

APRENDE A DESACTIVAR VENTANAS EMERGENTES

1. **Abre el buscador** en tu ordenador.
3. Haz clic en **Configuración avanzada**, que está en la parte inferior.
5. Haz clic en Ventanas emergentes y **redirect**.



2. Haz clic en el **Más** que está en la esquina superior derecha. **Configuración**.
4. En "Privacidad y seguridad", haz clic en **Configuración del sitio**.
6. Selecciona la opción **Permitido o Bloqueado** que está en la parte superior.

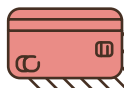
PHISHING

Engañar al usuario para robarle información confidencial haciéndole creer que está en un sitio de confianza.



OBJETIVOS DEL PHISHING

Contraseñas



Información bancaria

Dinero



Identidad

CONSEJOS PARA EVITAR EL PHISHING



- Verifica la fuente de tus emails.
- Nunca entres a tu banco a partir de un correo electrónico.
- Da tus datos personales únicamente en webs seguras.
- Periódicamente revisa tus cuentas, especialmente las bancarias.
- Si hay faltas ortográficas o está mal escrito, sospecha.
- Estate al día de las novedades del *malware*.
- Ante la duda, ignora el mensaje.

SEM



DÓNDE APARECE



Buscadores



YouTube



Redes sociales

RECOMENDACIONES PARA ACTUAR ANTE EL SEM



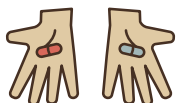
Evita las primeras opciones de los buscadores.



Ten en cuenta que también hay publicidad pagada en RRSS.



En RRSS a veces parecen *post* normales.



Aprende a identificar lo que es publicidad.



Ante todo, usa el sentido común.

PROTECCIÓN DE DATOS EN REDES SOCIALES

Las RRSS son cultivo para el tráfico de datos e información que no queríamos que se divulgue.



PRINCIPALES REDES SOCIALES



WhatsApp



Facebook



Instagram



LinkedIn



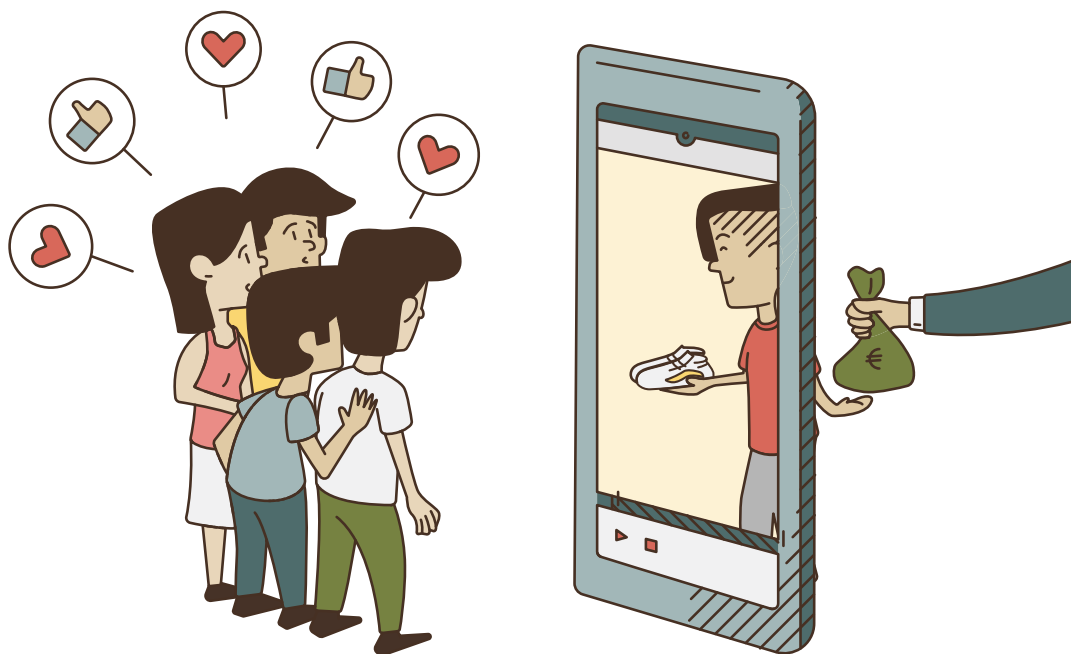
Twitter

RECOMENDACIONES

- No des nunca tus datos personales.
- No aceptes solicitudes de amistad de desconocidos.
- Define la privacidad de las fotos que subes.
- Configura la privacidad de tu perfil.
- Usa contraseñas seguras (con mayúsculas y minúsculas, números y símbolos).
- No uses la misma contraseña en distintas cuentas.
- Personaliza la privacidad de tu biografía.

INFLUENCERS

La publicidad siempre ha recurrido a caras conocidas y los influencers no son una excepción, pero raramente señalan su contenido como publicidad.



¿DÓNDE ACTUAN LOS INFLUENCERS?

- RRSS   
- Blogs 
- Youtube 

RECOMENDACIONES

- Infórmate sobre los productos que te interesan en medios fiables.
- Si dudas de un contenido, actúa como un consumidor crítico y responsable.
- Internet ofrece inmediatez. Recapacita antes de comprar.
- Aplica el sentido común.
- Las críticas negativas también pueden ser pagadas.

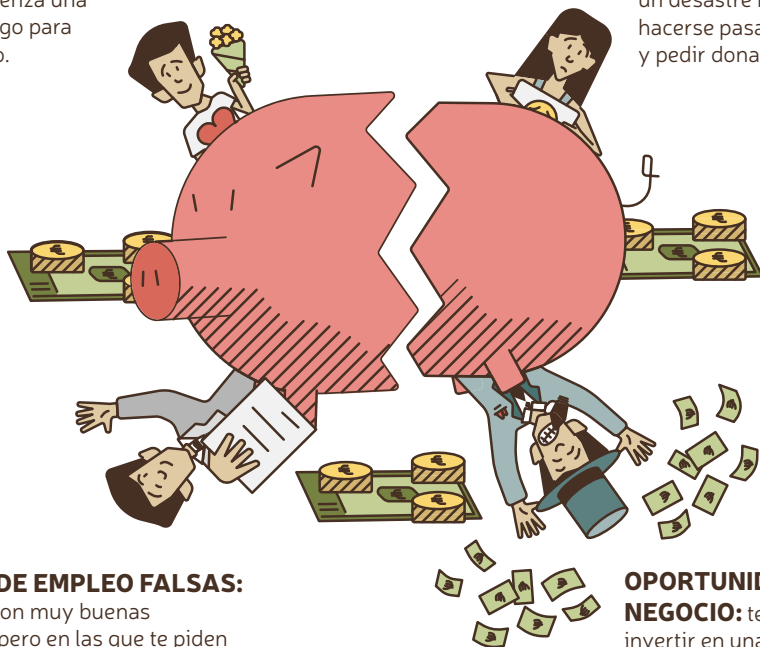
ENGAÑOS EN INTERNET

Podemos hacer casi cualquier cosa por Internet: conocer gente, comprar, invertir, etc. Pero hay que ser precavido porque debemos ser consumidores críticos y responsables porque hay estafadores que pretenden ganar dinero y obtener datos personales.

TIPOS DE ENGAÑOS MÁS FRECUENTES

SENTIMENTALES: una persona comienza una relación contigo para pedirte dinero.

CARIDAD: comunes tras un desastre natural, al hacerse pasar por una ONG y pedir donaciones.



OFERTAS DE EMPLEO FALSAS:

son ofertas con muy buenas condiciones pero en las que te piden dinero para tramitar papeles o enviarte documentación.

OPORTUNIDADES DE NEGOCIO:

te ofrecen invertir en una empresa y piden dinero para trámites o documentación.



RECOMENDACIONES PARA EVITAR FRAUDES

- No hables con la persona fuera de la web donde le has conocido.
- Pide una videollamada para ver si se hacen pasar por otra persona.
- Al hacer cualquier compra o pago, infórmate y lee opiniones de otras personas.
- Busca información sobre las empresa u ONGs.
- Desconfía si el precio es mucho más bajo del habitual.
- Asegúrate que las webs y tiendas online son legales.
- Acude a la fuente oficial, en vez de hacerlo por el enlace que te envían.
- Utiliza tarjetas de prepago o en las que tengas poco dinero.
- Consulta tu cuenta bancaria tras una compra por Internet.
- Conserva facturas y los correos electrónicos de tus compras.

PRIVACIDAD Y MÓVILES

Actualmente llevamos toda clase de información en nuestros dispositivos móviles, por lo que es fundamental evitar que expongan la integridad de nuestros datos e imágenes personales.

CÓMO PUEDEN ACCEDER A TUS DATOS



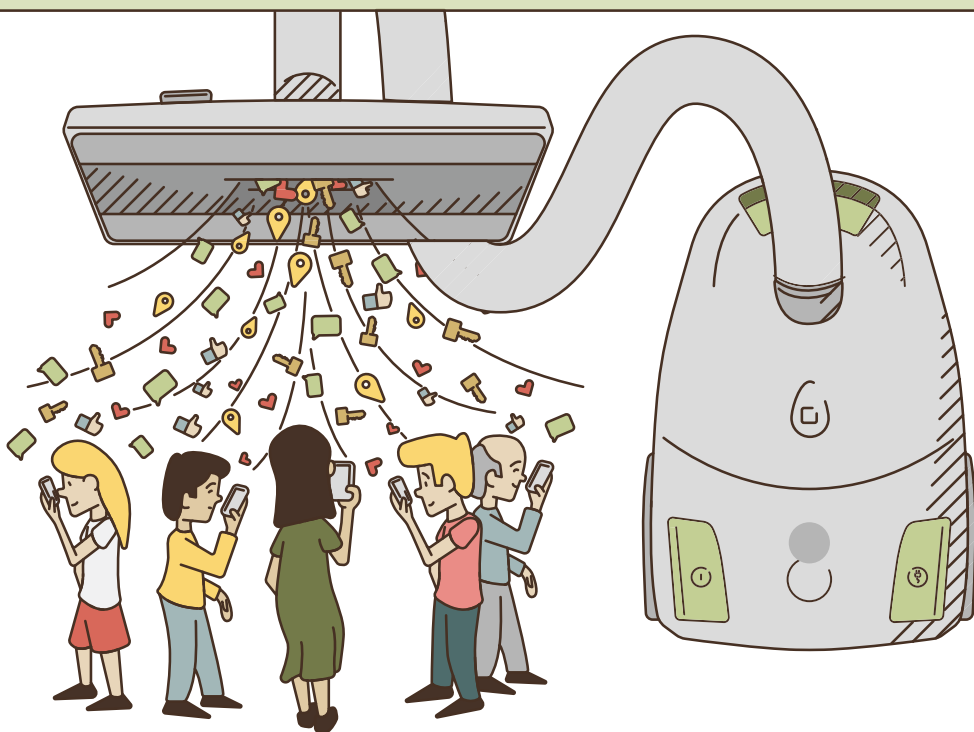
Redes WiFi públicas o comprometidas



Aplicaciones no oficiales



Links a contenidos dudosos



RECOMENDACIONES



Ten en cuenta los permisos que das a las aplicaciones.



Usa distintas contraseñas para las cuentas.



Limita la exposición a las redes sociales.



Usa un código de bloqueo de pantalla.



Cambia la contraseña cada cierto tiempo.



Actualiza tu software.



Usa un administrador de contraseñas.



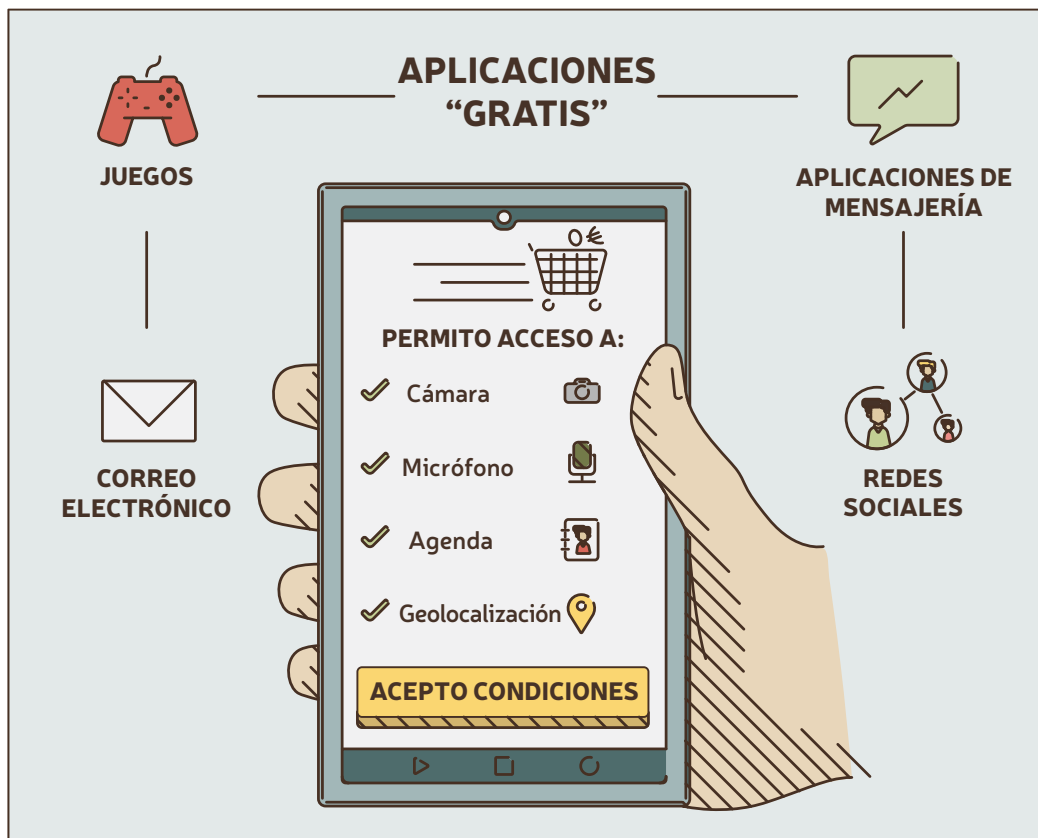
Investiga las aplicaciones que instalas.



Descarga aplicaciones solo de tiendas oficiales.

NADA ES GRATIS

Aplicaciones, RRSS o juegos aparentemente gratis, no lo son ya que si no se cobra por su uso, se cobrará en forma de consumo publicitario o incluso se comerciará con los datos personales.



RECOMENDACIONES



Aplica el sentido común. Crear una aplicación cuesta dinero y necesita rentabilizarse.



Revisa los permisos de las aplicaciones.



Revisa la privacidad de tus RRSS: quién puede acceder a tu contenido y etiquetarte.



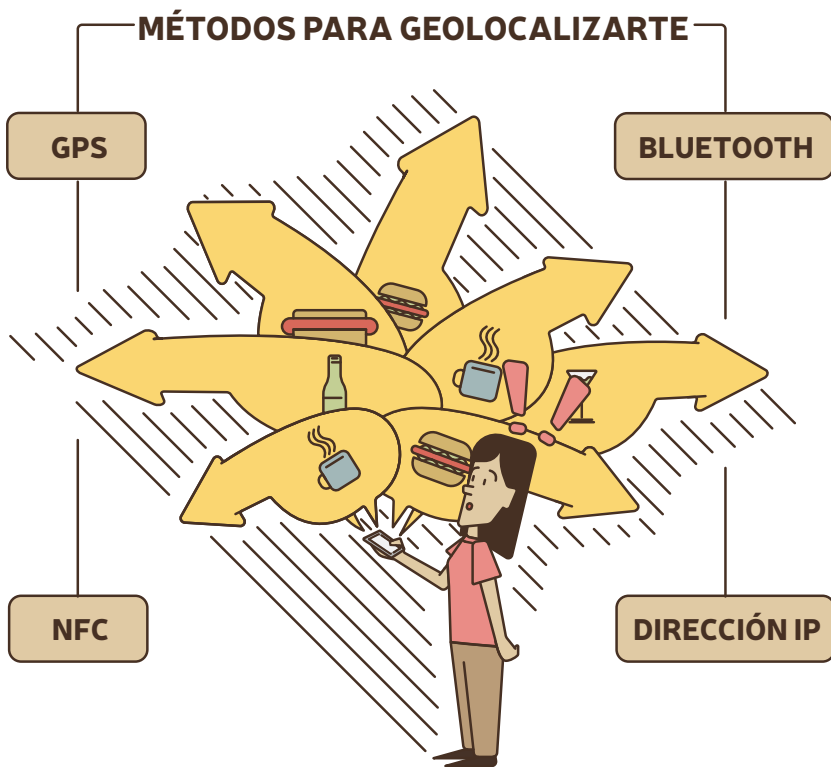
Comprueba qué información está publicada en Internet sobre ti y toma medidas.



No des datos privados en cualquier página web o aplicación.

GEOLOCALIZACIÓN

Algunos comercios geolocalizan a sus clientes y les envían notificaciones cuando se encuentran cerca de comercios para incitarles a que entren en sus locales.



RECOMENDACIONES

- Mantén apagado el *GPS*, *Bluetooth* y *NFC* en los momentos que no los necesites.
- Elimina los metadatos en la aplicación de fotografía.
- **Oculto la dirección IP en tu navegador.**
- **No aceptes las cookies de geolocalización en las webs.**
- Evita que tu navegador sepa tu localización.
- Oculta la IP de tu correo electrónico.
- Borra tus ubicaciones pasadas del navegador.

Acude a tu sede más cercana de ADICAE.
Obten más materiales y herramientas de aprendizaje sobre RRSS.
Conviértete en consumidor crítico, responsable y solidario.

www.adicae.net

Edita:

ADICAE, Asociación de Usuarios de Bancos, Cajas y Seguros.

Servicios Centrales.

C/ Gavín 12, local. 50001 Zaragoza.

Depósito legal: Z 2011-2019

Ilustración: Daniel Crespo.

Maquetación: Carolina Saiz.

Con el apoyo del Ministerio de Sanidad, Consumo y Bienestar Social.

Su contenido es responsabilidad exclusiva de la Asociación.

www.adicae.net



Adicae Consumidores



ADICAE



adicae_consumidores



ADICAE Consumidores



Con el apoyo del Ministerio de Sanidad, Consumo y Bienestar Social
Su contenido es responsabilidad exclusiva de la Asociación