Guía Android

EL CICLO DE VIDA SEGURO

DE LOS DISPOSITIVOS MÓVILES

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta

No te pierdas ningún detalle de la guía, accediendo a la versión digital.

ÍNDICE

Contenido **Página**

Licencia de Contenidos

0 INTRODUCCIÓN

El inmenso abanico de posibilidades que ofrecen los smartphones y tablets hace que cada vez estén más extendidos estos dispositivos entre los usuarios. Sin embargo, no están exentos de riesgos, ya que, por ejemplo, se pueden estropear, ser robados o incluso perderse, derivando en la pérdida y control de la información que se tiene almacenada en ellos.

Además, si te detienes unos segundos a pensar, podrás darte cuenta de todo lo que tus dispositivos conocen sobre ti: quiénes son tus contactos, aplicaciones que utilizas, lugares favoritos que frecuentas, páginas web que visitas, credenciales que utilizas para acceder a tus cuentas, fotografías y vídeos que grabas, etc.

Impresiona, ¿verdad?

Ahora bien,

¿Qué pasa si alguien accede a esa información sin tu consentimiento?

¿O si pierdes o te roban el dispositivo?

¿O si se estropea?

No te preocupes, gracias a esta guía aprenderás a usar y configurar tus dispositivos de forma segura, teniendo en cuenta una serie de consideraciones básicas y protegiendo siempre tu información para que, pase lo que pase, no la pierdas ni esté disponible para terceros que intenten consultarla.

Nota: Las distintas configuraciones que encontrarás en esta guía están basadas en la versión Android 10. Además, ten en cuenta que, dependiendo del fabricante de tu dispositivo, los literales o ubicaciones de las distintas opciones que te mostraremos pueden ser ligeramente diferentes.

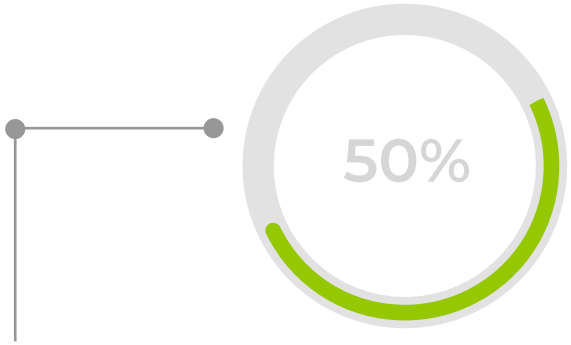
1 MÓVIL NUEVO EN LA MANO ¿Y AHORA QUÉ?

Elige un idioma | Conéctate a una red wifi | Vincula tu cuenta de Google | Actualiza el software

Elige un idioma:
El primer paso que debes realizar es seleccionar el idioma. Seleccionando el país, la configuración de fecha y hora se ajustará automáticamente.

Conéctate a una red wifi:
Aunque el siguiente paso no es obligatorio para continuar, es recomendable que configures tu red wifi en este momento para facilitar los siguientes pasos de la configuración de tu móvil. Asegúrate de conectarte a una red wifi segura (evita redes públicas y gratuitas).

- Selecciona tu **red wifi e introduce tu contraseña**.



Vincula tu cuenta de Google:

- Si ya dispones de una cuenta de Google, solo deberás introducir tus credenciales de Gmail.
- Si no dispones de una cuenta Gmail, puedes crearla más tarde desde el panel de **Ajustes** dentro de **Cuentas y sincronización.**

La importancia de activar tu cuenta personal de Google radica en los beneficios que te ofrece la compañía. Por ejemplo, la descarga de aplicaciones gratuitas o de pago desde su tienda virtual o poder encontrar tu móvil en caso de pérdida.

Actualiza el *software*:
Las versiones de Android siempre están actualizándose. Antes de comenzar a utilizar tu nuevo móvil, actualízalo a la última versión.
Podras hacerlo en **Ajustes > Acerca del teléfono > Actualización de *software* > Descargar actualización**

No te olvides de mantener el software actualizado. De este modo tendrás tu dispositivo protegido ante posibles fallos de seguridad que puedan aparecer.

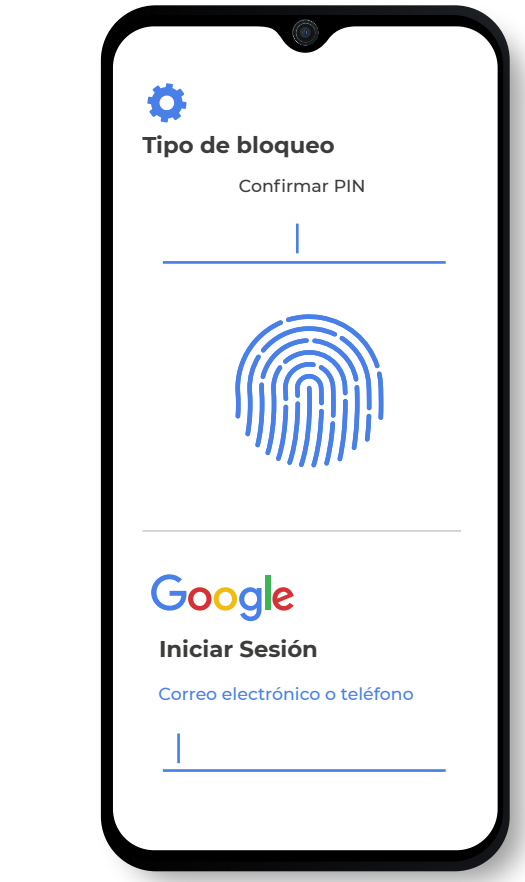
2 ¡QUÉ NADIE LO USE... SIN TU PERMISO!

Establece contraseñas seguras | Doble factor de autenticación

Establece contraseñas seguras:
Dispones de varias medidas de seguridad para bloquear tu dispositivo e impedir que terceras personas puedan hacer uso de él. ¡Gestiona tus contraseñas y resto de medidas de manera segura!

- **Código PIN:** ve a **Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla** y selecciona tu PIN.
- **Contraseña alfanumérica:** dirígete a **Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla > Contraseña**. Te pedirá introducir una contraseña que contenga al menos cuatro caracteres.
- **Patrón de desbloqueo:** accede a **Ajustes > Seguridad y Ubicación > Bloqueo de Pantalla** (al igual que el PIN) y selecciona el patrón de desbloqueo.
- **Huella dactilar:** acude al menú anterior: **Ajustes > Seguridad y Ubicación > Huella digital**. Desde aquí, sigue los pasos necesarios para terminar de configurarla.
- **Desbloqueo por reconocimiento facial:** ve a **Ajustes > Seguridad y Ubicación > Smart lock > Reconocimiento Facial**. A partir de aquí, el sistema te guiará para terminar la configuración.

INTRODUCE LA CONTRASEÑA



Doble factor de autenticación:
Además del uso de una contraseña, añade una capa adicional de seguridad a tu cuenta de Google para que si alguien captura o adivina tu clave de acceso, no pueda acceder a ella. ¿Cómo activar la verificación en dos pasos?
Ve a **Ajustes > Google > Gestionar tu cuenta de Google > Seguridad**. En Inicio de sesión de Google pulsa Verificación en dos pasos > Empezar y sigue los pasos indicados.

3 CONEXIONES SIEMPRE SEGURAS

Configuraciones de redes inalámbricas

Configuraciones de redes inalámbricas

- **Wifi:**
  Mediante esta opción podrás conectarte a redes wifi que se encuentren dentro del rango del dispositivo. Para ello: **En Ajustes > Wi-Fi** verás las redes disponibles.
  Haz clic en una de las redes de la lista. Si se necesita una contraseña, verás el icono del candado.
  La red se guardará y siempre que tu teléfono esté cerca y la **conexión Wi-Fi activada**, se conectará automáticamente.

  Recuerda: evita el uso de redes wifi públicas y, si por alguna razón tienes que hacerlo, no accedas a tus cuentas o servicios para que no se hagan con tus credenciales de acceso.

- **Crear un punto de acceso wifi:**
  Un punto wifi te permitirá compartir tus datos de Internet con quien quieras. Para ello:
  Accede a **Ajustes** y selecciona la opción **Más o Más redes.**
  Allí encontrarás **Compartir Internet y Zona Wifi** o, en algunos casos, **Zona Portátil.**
  A continuación, activa la pestaña correspondiente.
  Luego tendrás que ponerle un **nombre a tu punto de acceso y una clave** para que los otros dispositivos puedan acceder. Solo será necesario hacer esto una vez, luego podrás activarla y desactivarla cuando quieras.

  Cuando termines de compartir tus datos, apaga esta función para que no sea utilizada por alguien más sin tu autorización.

- **Bluetooth:**
  Para configurar el Bluetooth de tu Android dirígete a: **Ajustes > Bluetooth** enciéndelo y verás una lista de dispositivos disponibles para conectar.
  Al vincular un dispositivo, te pedirá permiso para emparejar los dispositivos. Puede darle en aceptar o permitir.

  Una vez hayas terminado de utilizarlo, desactívalo. Así evitarás que terceros puedan llegar a conectarse y robar información personal como fotos o vídeos o transferirnos algún archivo malicioso a nuestro dispositivo.

- **NFC:**
  Para activar el NFC de tu móvil deberás:
  Ingresar en **Ajustes > Redes,** y busca **NFC**.
  Desliza la pestaña para activarlo. Ahora podrás compartir tus datos con solo tocar otro dispositivo o realizar pagos con tu dispositivo móvil. No está de más recordarte que el dispositivo al que quieras enviar la información deberá tener activo el NFC.

  Utilizarás esta tecnología principalmente para realizar pagos sin necesidad de usar tarjetas físicas. Infórmate sobre cómo hacerlos con NFC de manera segura.

  Una vez que hayas terminado, recuerda cerrar la aplicación. Un tercero podría realizar algún cargo a tu tarjeta si no tienes cuidado.

4 PROTECCIÓN CONTRA VIRUS Y FRAUDES

Antivirus | Actualización de software

Antivirus:
Tu dispositivo no está exento de riesgos de infectarse por algún virus a través de una app o al descargarte un archivo infectado. Para protegerlo:

- Selecciona un antivirus directamente desde la tienda oficial Play Store, asegurándote de que previamente lees las reseñas de este.
- Haz clic en **Obtener**. Es posible que tengas que iniciar sesión con tu ID de Google.
- Abre la app y configúrala para mantener tu dispositivo Android libre de virus

Disponible en
Google Play

Actualización de *software*:
Durante la vida útil del sistema operativo, los desarrolladores van descubriendo errores y fallos de seguridad que necesitan ser solucionados. Sin actualizaciones, tu dispositivo estaría más expuesto y vulnerable frente a los ataques de los ciberdelincuentes.

- Si no has recibido la notificación de que existe una actualización nueva o quieres revisar si está actualizado o no, dirígete a **Ajustes > Información del teléfono > Actualizaciones del sistema/*software* > Comprobar actualizaciones** y comprueba si tienes la última versión.

Otras herramientas de protección:
Además de con antivirus, blinda el acceso a tu información con aplicaciones de bloqueo de apps, gestores de contraseñas, función de verificación en dos pasos o que protegen tu privacidad, entre otras.

5 ¡NO PIERDAS TU INFORMACIÓN Y PROTÉGELA!

Copias de seguridad | Cifrado

Nuestro dispositivo móvil no es solo una extensión de nosotros, también se convierte en una unidad de almacenamiento de toda nuestra vida. Imagina que un día lo perdieses...

¿Podrías recuperar toda la información almacenada en él?

Para minimizar riesgos, lo mejor es hacer copias de seguridad:

Copias de seguridad en la nube de Google: Android tiene su propio sistema de copias de seguridad en la nube (Google Drive), para hacer uso de él:

- Ve a **Ajustes > Google > Hacer copia de seguridad.**
  Si está desactivada (que lo estará si has desmarcado la opción en la configuración inicial), actívala.
- A continuación, selecciona **Crear una copia de seguridad.**

Cifrado:
No te olvides del cifrado del teléfono y su información, una **medida adicional de seguridad** para que, en caso de perder nuestro dispositivo, los datos no acaben en malas manos.

- En las últimas versiones de sistema operativo Android, el teléfono viene cifrado por defecto, no obstante, si tienes una memoria externa del almacenamiento, deberás cifrarla desde el menú **Ajustes > Seguridad y Ubicación > Cifrar almacenamiento de tarjeta SD.**

6 PERSONALIZACIÓN ¡HAZLO TUYO!

Instalación de apps desde Play Store | Permisos de apps | Geolocalización

Juegos, música, vídeos y muchísimos más tipos de apps están a tu disposición para instalar en tu dispositivo móvil. En cuestión de segundos tendrás instaladas todas las apps que quieras, pero ¡ojo!, las apps se instalan en tu dispositivo y acceden a determinadas funcionalidades a través de permisos. Si la app no es del todo fiable, puede hacer un mal uso de estos permisos y poner en riesgo tu seguridad y privacidad.

Instalación de apps desde Play Store:
Para instalar apps en tu dispositivo Android, debes dirigirte a la tienda oficial de Google Play Store que ya viene instalada por defecto.

- Busca la app que quieras instalar y haz clic en **Instalar**. No te olvides de revisar los comentarios y valoración de otros usuarios. Aunque esté en la tienda oficial, es importante informarse bien sobre la app.

Google Play

Permisos de apps:
Cuando una app pide permisos, está solicitando acceso a alguna funcionalidad de tu dispositivo. Revisa con mucha atención si tiene sentido que pida un permiso determinado y, si quieres revisar o administrar los permisos de las apps ya instaladas:

- Ve a **Ajustes > Aplicaciones,** donde verás una lista de todas las apps instaladas.
- A continuación, selecciona la app cuyos permisos quieras administrar.
- A continuación, haz clic en **Permisos** desde donde podrás activar y desactivar los permisos que consideres.

Geolocalización:
La función de geolocalización permite obtener información basada en la ubicación del dispositivo y ofrece predicciones sobre tus desplazamientos, restaurantes cercanos, etc. Aunque puede resultar muy útil, puedes sentir que tu privacidad está siendo invadida ya que estos datos se comparten con Google.

- Para desactivarla ve a **Ajustes > Ubicación > Utilizar ubicación.**

7 ¡LOCALIZA TU DISPOSITIVO!

Desde web

Supón que has perdido tu dispositivo. No te preocupes, existe una función para localizarlo esté donde esté.

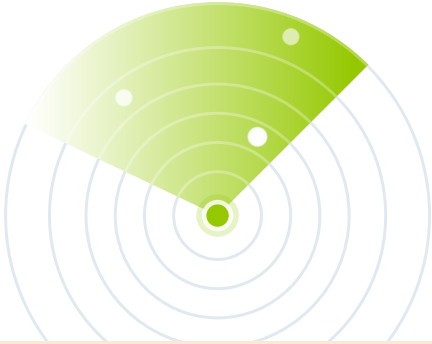
Si has ingresado a tu Android con la cuenta de Google, **es posible que ya tengas por defecto la geolocalización activada**, a no ser que la hayas desactivado previamente. Hay que tener en cuenta las siguientes condiciones que se deben cumplir para que la búsqueda sea efectiva:

- El móvil deberá estar encendido en el momento de buscarlo.
- Tu **cuenta Google** deberá estar activa en el móvil.
- El móvil deberá estar conectado a una red wifi o con datos móviles.
- El servicio de ubicación o GPS del móvil deberá encontrarse en modo **Activado**.
- Y algo muy importante, que no hayas desactivado la herramienta **Encontrar mi dispositivo**.

Desde la **web**, puedes hacerlo de la siguiente forma:

- Accede a tu cuenta de Google.
- Haz clic en el apartado de **Seguridad**.
- En **Tus dispositivos** encontrarás la opción **Buscar un dispositivo perdido**.
- **Selecciona el dispositivo** que quieres localizar y listo.

Esta función es muy útil, pero no olvides proteger tu cuenta adecuadamente, con una contraseña robusta y activando la verificación en dos pasos, para evitar que otra persona acceda a ella y localice la ubicación de tu dispositivo, y la tuya.



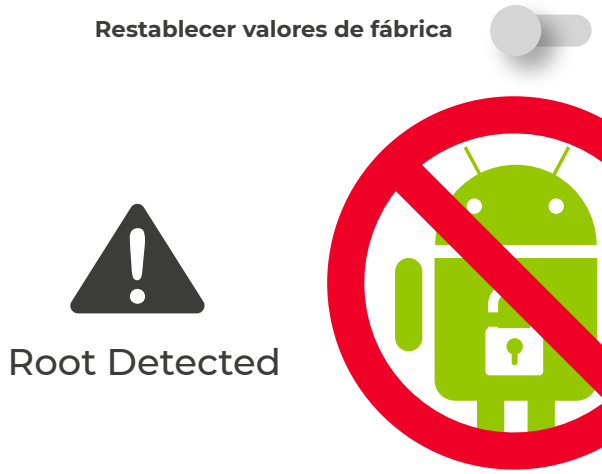
8 YA PASARÁ A OTRA VIDA DESHACERNOS DEL MÓVIL

Borrado seguro

Borrado seguro:
Si tu dispositivo se ha quedado anticuado y quieres deshacerte de él por uno nuevo, ¡no lo tires sin más! Aunque creas haber eliminado todo rastro de tu información, es posible que aún pueda recuperarse si cae en malas manos. Para hacer un borrado seguro de toda tu información personal, deberás hacer lo siguiente:

- Si tu dispositivo tiene una tarjeta microSD, debes **cifrar la tarjeta microSD y formatearla**. Ve a **Ajustes > Seguridad > Cifrar tarjeta SD** y a continuación, para formatearla, dentro del menú de Ajustes pulsa en **Almacenamiento > Tarjeta SD > Formatear.**
- Elimina todas las cuentas enlazadas como la de Google, dirigiéndote a **Ajustes > Cuentas > [seleccionamos la cuenta] > Eliminar.**
- Restaura los valores de fábrica. Ve a **Ajustes > General > Restablecer datos de fábrica > Restablecer.** Quizás debas usar el buscador para encontrar la opción de restablecer datos de fábrica, puesto que dependiendo del fabricante puede encontrarse en otro menú.

Si al dispositivo se le había hecho un *rooting*, la opción de restablecer podría no funcionar correctamente. En ese caso, tendrás que acudir a un técnico especializado. Se conoce como *rooting* al proceso de eliminar las limitaciones impuestas por el desarrollador en un dispositivo Android. Esta práctica no es recomendable para usuarios no técnicos.



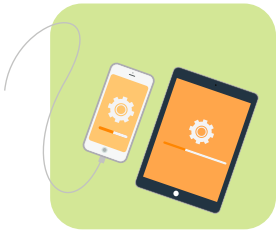
PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD

9 CONSEJOS GENERALES

1. Vincula tu dispositivo móvil a una cuenta Google en tu móvil Android.
2. Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una contraseña robusta.
3. Activa el sistema de actualizaciones automáticas de tu dispositivo y aplicaciones, pues con esto se corrigen los defectos en seguridad que puedan tener.
4. Usa aplicaciones de seguridad que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.
5. Protege tu información mediante copias de seguridad. De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.

6. Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).
7. Cuando instales aplicaciones, revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios. ¡Y acuérdate de eliminar las que ya no uses!
8. Otorga los permisos a las apps que sean imprescindibles para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.
9. Evita prácticas de riesgo con el rooting en Android.
10. Si vas a deshacerte de tu móvil, asegúrate de borrar toda la información que contiene para no dejar rastro.
11. Apóyate en herramientas de control parental si el dispositivo lo va a utilizar un menor.

10 ENLACES DE INTERÉS



Dispositivos móviles

La 2ª vida de nuestros dispositivos

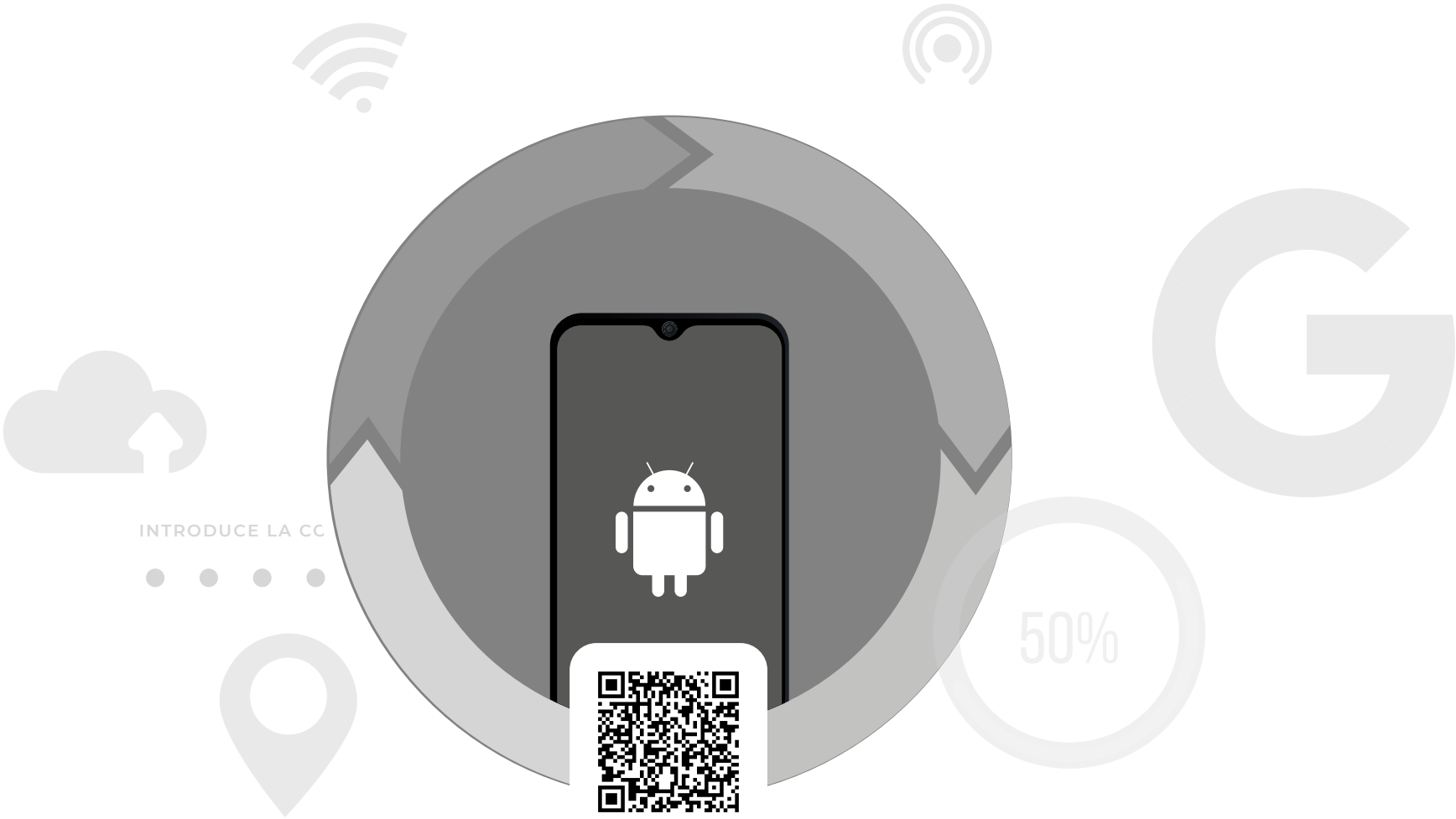
¿Cuánto valen mis datos en la Red?

¡Contraseñas seguras!

Ingeniería social: que no te engañen

Puesta a punto para el nuevo curso

No te pierdas ningún detalle de la guía, accediendo a la versión digital.



No te pierdas ningún detalle de la guía, accediendo a la versión digital con este QR.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
OSI Oficina de Seguridad del Internauta