incibe_ emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#INCIBEemprende

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

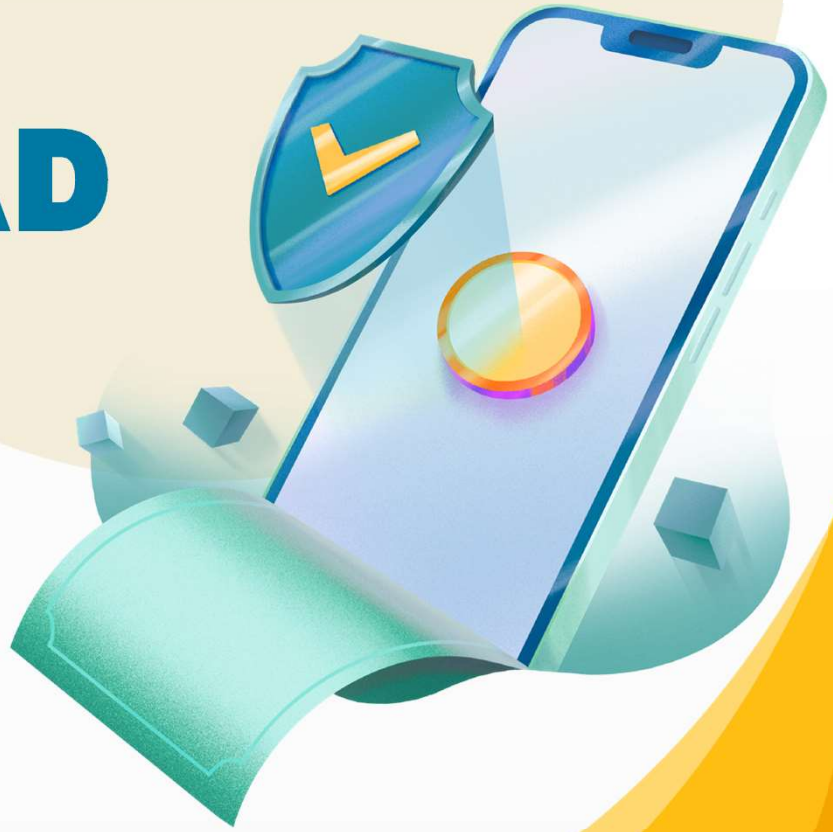
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

DRAPER B1

CIBERSEGURIDAD EN TU BOLSILLO

PROTEGE TU SMARTPHONE



Colabora:

AYUNTAMIENTO DE TORREVIEJA

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

ÍNDICE

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

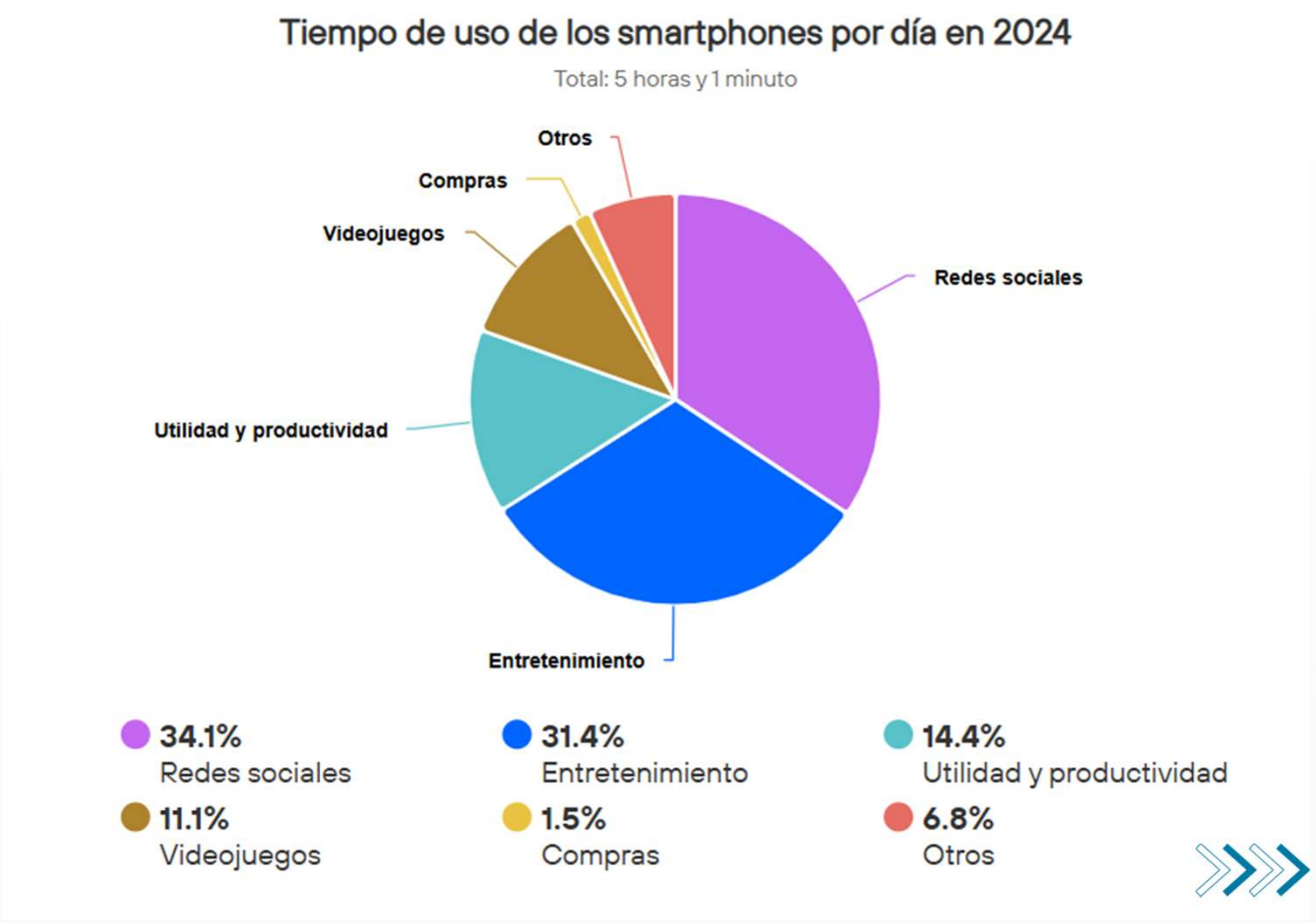
Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

¿POR QUÉ HAY QUE PROTEGER NUESTRO SMARTPHONE?

¿CUÁNTO USAMOS EL MÓVIL?



FEB 2025

MOBILE CONNECTIVITY

USE OF MOBILE PHONES AND DEVICES THAT CONNECT TO CELLULAR NETWORKS

SPAIN

NUMBER OF CELLULAR MOBILE CONNECTIONS (EXCLUDING IOT)

56.1

MILLION

NUMBER OF CELLULAR MOBILE CONNECTIONS COMPARED WITH TOTAL POPULATION

117%

YEAR-ON-YEAR CHANGE IN THE NUMBER OF CELLULAR MOBILE CONNECTIONS

-7.0%

-4.2 MILLION

SHARE OF CELLULAR MOBILE CONNECTIONS THAT ARE BROADBAND (3G, 4G, 5G)

98.3%

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

FEB 2025

SHARE OF MOBILE WEB TRAFFIC BY MOBILE OS

PERCENTAGE OF WEB PAGE REQUESTS ORIGINATING FROM MOBILE HANDSETS RUNNING EACH MOBILE OPERATING SYSTEM IN DECEMBER 2024

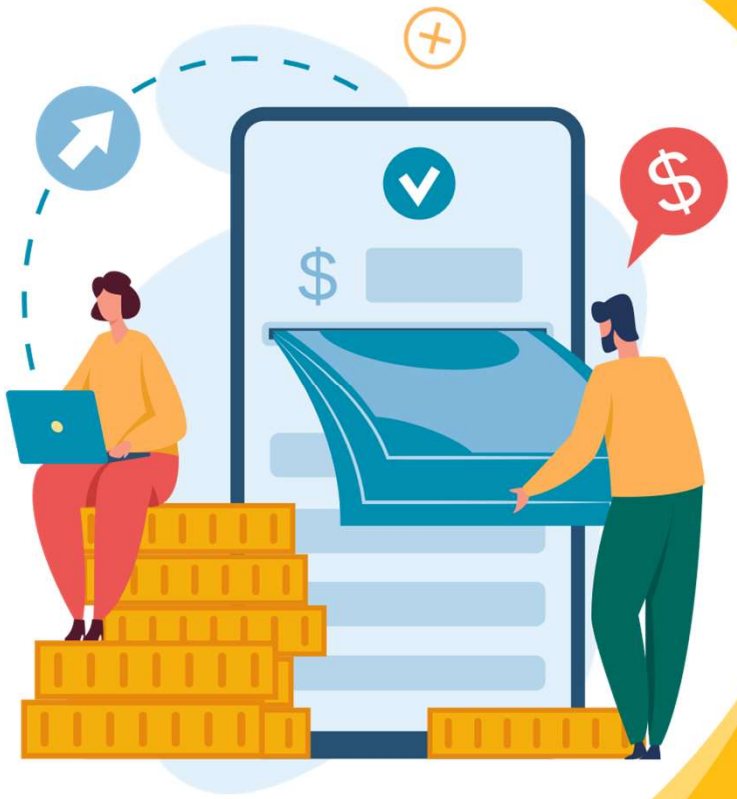
SPAIN

Más tasa de adopción,
más propenso a ser atacado

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

¿POR QUÉ HAY QUE PROTEGER NUESTRO SMARTPHONE?

Tú móvil es tu vida digital



Tu teléfono no solo es un aparato, es tu banco, tu correo, tus redes sociales, tus fotos, tu identidad. Es tu cámara, tu agenda, tu GPS, tu álbum familiar, tu historial médico y hasta tu cartera.

Un sólo acceso indebido puede significar el robo total de tu vida digital.

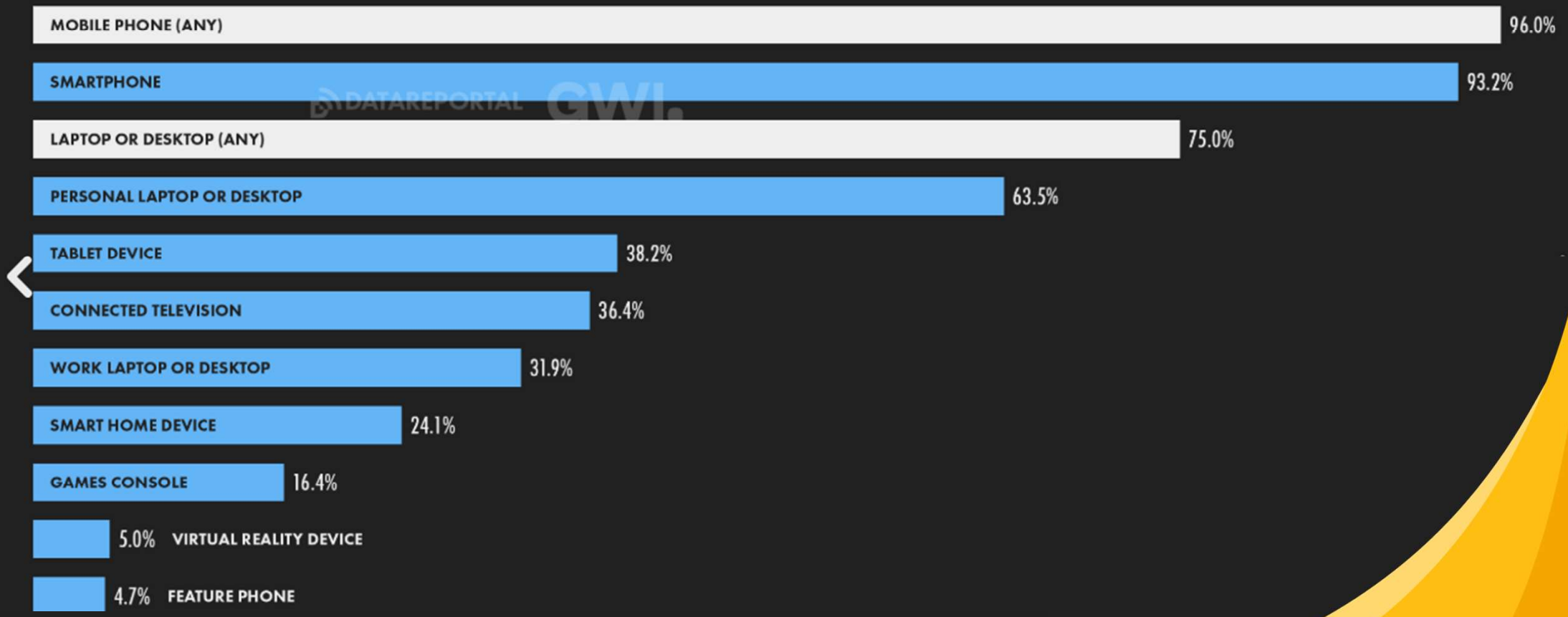
Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

FEB 2025

DEVICES USED TO ACCESS THE INTERNET

PERCENTAGE OF INTERNET USERS AGED 16+ WHO USE EACH KIND OF DEVICE TO ACCESS THE INTERNET

SPAIN



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

¿POR QUÉ HAY QUE PROTEGER NUESTRO SMARTPHONE?

El riesgo está creciendo

Durante el año pasado, se detectaron **más de 33,3 millones de ataques a usuarios de smartphones** en todo el mundo, que involucraron varios tipos de malware y software no deseado.

La amenaza más común para los dispositivos móviles fue el **adware** (35% de todas las amenazas detectadas).

iOS más expuesto a ataques de phishing que Android: En 2024, el 18,4% de los dispositivos iOS enfrentaron ataques de phishing, en comparación con el 11,4% de los dispositivos Android.

Incremento del 196% en **ataques con troyanos bancarios en Android**: En 2024, los ataques con troyanos bancarios en dispositivos Android aumentaron de 420.000 en 2023 a 1.242.000 en 2024.

Informe de Kaspersky "The Mobile Malware Threat Landscape in 2024"

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

ANDROID VERSUS IOS

Teléfonos con sistema operativo Android

- **Pro:** altamente configurable; puedes controlar totalmente la configuración de privacidad.
- **Contra:** la falta de estandarización implica una seguridad lista para usar débil.
- **Sugerencia:** mejor si te sientes cómodo con el ajuste de la configuración y las herramientas de seguridad.

Teléfonos Apple (iOS)

- **Pro:** coherencia y fiabilidad; sabes lo que vas a obtener.
- **Contra:** no es invulnerable al malware; depende en gran medida de la práctica de seguridad de Apple. Además, aunque los productos de Apple generalmente tienen un precio superior a los de Android, no garantizan una seguridad total y siguen siendo vulnerables al malware y el pirateo.
- **Sugerencia:** probablemente la opción más sencilla para una seguridad "bastante buena".

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

¿POR QUÉ HAY QUE PROTEGER NUESTRO SMARTPHONE?

La confianza nos vuelve vulnerables

El 90% de las personas no tienen ningún tipo de protección activa en su móvil.

No necesitas ser experto para protegerte: Basta con aplicar prácticas simples.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Herramientas de seguridad para proteger un dispositivo móvil

Descubre cuáles son las aplicaciones que fortalecerán la seguridad de tu dispositivo

Antivirus: detectan aplicaciones maliciosas que podamos descargar.

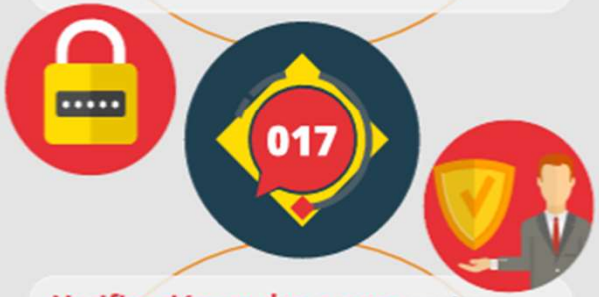
- **Google Play Protect:** incluida por defecto en dispositivos Android. Revisa automáticamente todas las aplicaciones instaladas con el objetivo de prevenir riesgos y garantizar la seguridad.
  - **Google Play > Menú (icono perfil) > Play Protect**
- **Modo de aislamiento:** protección de seguridad adicional para dispositivo iOS. Recomendado para usuarios que puedan ser objetivo de ataques sofisticados.
  - **Ajustes > Privacidad y seguridad > Modo de aislamiento**

Gestor de contraseñas: almacena y gestiona las claves de forma segura, crea contraseñas robustas y permite la sincronización con otros dispositivos.

- **Contraseñas:** aplicación nativa para iOS.
  - **Ajustes > Contraseñas**
- **Gestor de contraseñas Chrome:** Se almacenan en tu cuenta de Google.
  - **Menú (icono tres puntos) > Configuración > Gestor de Contraseñas**

Bloqueo de publicidad: diseñado para bloquear los anuncios que se muestran en las páginas web.

- **Bloqueador de anuncios de Chrome para Android:**
  - Configuración > Configuración avanzada > Configuración de sitios > Anuncios invasivos
- **Bloqueador de anuncios de Safari en iOS:**
  - Ajustes > Safari > Bloquear ventanas
  - Ajustes > Safari > Aviso de sitio web fraudulento



Antirrobo: ayuda a encontrar el dispositivo perdido o robado. Además, proporciona funciones como el borrado remoto de la información.

- **Encontrar mi dispositivo:** aplicación nativa para Android.
  - Ajustes > Google > Encontrar mi dispositivo
- **Buscar:** aplicación nativa para iOS.
  - Ajustes > Nombre de usuario > Buscar

Verificación en dos pasos: protege las cuentas al generar un código de un solo uso que habrá que introducir en el proceso de login.

- **Google Authenticator:** disponible para su descarga en Google Play y Apple Store.
- **Microsoft Authenticator:** disponible para su descarga en Google Play y Apple Store.

Bloqueo de llamadas: realiza un filtrado de las llamadas entrantes para evitar las que no nos interesan.

- **Filtrar llamadas no deseadas:** opción nativa para Android.
  - Desde la app Teléfono > Ajustes > Identificación de Llamadas y Spam
- **Identificación de llamadas:** opción nativa para iOS.
  - Ajustes > Teléfono > Mostrar ID de llamad

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

ANTIVIRUS

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

Antivirus: detectan aplicaciones maliciosas que podamos descargar.

- **Google Play Protect:** incluida por defecto en dispositivos Android. Revisa automáticamente todas las aplicaciones instaladas con el objetivo de prevenir riesgos y garantizar la seguridad.
  - **Google Play > Menú (icono perfil) > Play Protect**

- **Modo de aislamiento:** protección de seguridad adicional para dispositivo iOS. Recomendado para usuarios que puedan ser objetivo de ataques sofisticados.
  - **Ajustes > Privacidad y seguridad > Modo de aislamiento**

ANTIVIRUS PARA SUMAR PROTECCIÓN

Android cuenta con funciones como **Google Play Protect**, que analiza aplicaciones en busca de malware antes y después de la instalación.
Si bien Android tiene funciones de seguridad integradas, las aplicaciones antivirus pueden ofrecer capas adicionales de protección, especialmente en redes públicas o al descargar aplicaciones de fuentes no confiables.

Aplicaciones de seguridad recomendadas:

- **AVG AntiVirus Free:** Ofrece análisis antivirus, protección en tiempo real y protección de navegación web.
- **McAfee Mobile Security:** Incluye VPN, análisis de redes Wi-Fi, protección de navegación y protección antivirus.
- **Avast Mobile Security:** Ofrece análisis antivirus, protección contra malware, protección de redes Wi-Fi y otras herramientas de seguridad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

IOS ECOSISTEMA CERRADO

iOS es conocido por su ecosistema cerrado, lo que hace que sea más difícil que el malware infecte los dispositivos.
iOS cuenta con funciones de seguridad robustas, como la **app de Sandbox** que limita el acceso de las aplicaciones a los datos del sistema, y actualizaciones frecuentes para corregir vulnerabilidades. Aunque iOS es más seguro que Android, las apps de antivirus pueden ser útiles para proteger contra amenazas específicas, como ataques de phising o malwares sobre todo en redes wi-fi públicas.

Aplicaciones de seguridad recomendadas:

- **Norton Mobile Security:** Ofrece análisis de seguridad, protección contra phishing y análisis de invitaciones a eventos para detectar enlaces peligrosos.
- **Avast Mobile Security:** Similar a la versión de Android, ofrece análisis antivirus, protección contra malware y protección de redes Wi-Fi.
- **McAfee Mobile Security:** Ofrece VPN, protección de navegación y análisis de redes Wi-Fi.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

CLAVES

- Los teléfonos Android e iOS no vienen con un antivirus instalado de serie, pero están protegidos por otras soluciones de seguridad integradas en el sistema operativo.
- Las aplicaciones de antivirus de terceros son una capa extra de seguridad que pueden servir para analizar ficheros descargados o detectar amenazas durante la navegación en internet.
- Recuerda descargar de tiendas oficiales (Google Play y App Store), revisa los comentarios y opiniones de usuarios, fíjate en quien es el desarrollador y el número de descargas.
- Para proteger nuestros teléfonos, lo más importante es mantener buenas prácticas de ciberseguridad, como no descargar aplicaciones fuera de las tiendas oficiales o mantener el sistema actualizado y el antivirus actualizado y realizar análisis periódicamente en tu móvil.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

GESTOR DE CONTRASEÑA

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

Gestor de contraseñas: almacena y gestiona las claves de forma segura, crea contraseñas robustas y permite la sincronización con otros dispositivos.

- **Contraseñas:** aplicación nativa para iOS.
  - **Ajustes > Contraseñas**

- **Gestor de contraseñas Chrome:** Se almacenan en tu cuenta de Google.
  - **Menú (icono tres puntos) > Configuración > Gestor de Contraseñas**

QUÉ OFRECEN LOS SISTEMAS OPERATIVOS POR DEFECTO

iOS: incluye **iCloud Keychain**, que almacena contraseñas, tarjetas y códigos de 2FA. Se sincroniza automáticamente entre dispositivos Apple, funciona muy bien si usas todo el ecosistema (iPhone, iPad, Mac)

Android (Google): integra **Google Password Manager**, sincronizado con tu cuenta de Google. Se activa desde Chrome o el sistema, y permite autocompletar en apps y webs.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

VENTAJAS DE USAR GESTORES EXTERNOS

- Usas múltiples sistemas (Android + Windows, iPhone + PC, etc.).
- Quieres compartir contraseñas de forma segura con otras personas (por ejemplo, familia o trabajo).
- Buscas funciones avanzadas como auditoría de contraseñas, notas seguras, autodestrucción remota, claves de acceso biométrico.

Recomendaciones con buena compatibilidad multiplataforma

- **Bitwarden:** Gratuito y de código abierto, con app en ambas plataformas, extensión para navegadores y versión web.
- **1Password:** Muy seguro, ideal para usuarios avanzados y familias.
- **NordPass:** Del equipo de NordVPN, centrado en usabilidad.
- **Dashlane:** Sencillo, interfaz muy intuitiva, ideal para principiantes.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

CLAVES

- Un gestor de contraseñas guarda todas tus claves de forma segura y solo necesitas recordar una.
- Activa el autocompletado para mayor comodidad, pero siempre con bloqueo biométrico.
- No uses el bloc de notas o similar para guardar contraseñas. Haz copias de seguridad de tu bóveda de contraseña y protégela con autenticación en 2 pasos.
- Tu contraseña maestra debe ser larga y única.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

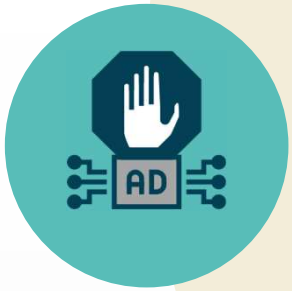
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1



BLOQUEO DE PUBLICIDAD Y LLAMADAS

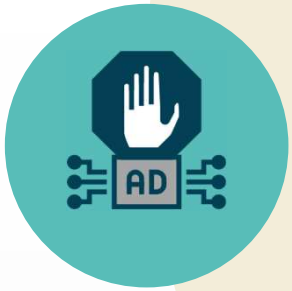
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1



Bloqueo de publicidad: diseñado para bloquear los anuncios que se muestran en las páginas web.

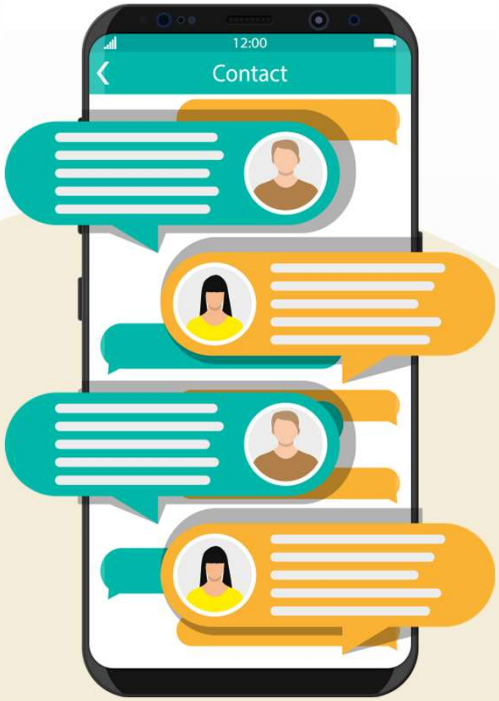
- **Bloqueador de anuncios de Chrome para Android:**
  - Configuración > Configuración avanzada > Configuración de sitios > Anuncios invasivos
- **Bloqueador de anuncios de Safari en iOS:**
  - Ajustes > Safari > Bloquear ventanas
  - Ajustes > Safari > Aviso de sitio web fraudulento

Bloqueo de llamadas: realiza un filtrado de las llamadas entrantes para evitar las que no nos interesan.

- **Filtrar llamadas no deseadas:** opción nativa para Android.
  - Desde la app Teléfono > Ajustes > Identificación de Llamadas y Spam
- **Identificación de llamadas:** opción nativa para iOS.
  - Ajustes > Teléfono > Mostrar ID de llamad

BLOQUEO DE PUBLICIDAD Y LLAMADAS

Además de virus y fraudes, los anuncios maliciosos y llamadas no deseadas son amenazas que podemos bloquear. Estas funciones te ayudan a evitar molestias y posibles estafas telefónicas. Son gratuitas y muy fáciles de activar.



Bloqueo de publicidad:

- En Android: activa el bloqueador de anuncios en Chrome desde Configuración > Configuración de sitios > Anuncios invasivos.
- En iOS: en Safari, ve a Ajustes > Safari > Bloquear ventanas y Aviso de sitio web fraudulento.

Bloqueo de llamadas no deseadas:

- En Android: Teléfono > Ajustes > Identificación de llamadas y spam.
- En iOS: Ajustes > Teléfono > Mostrar ID de llamada.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

VERIFICACIÓN EN 2 PASOS

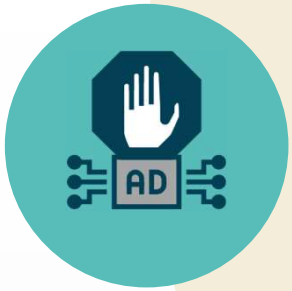
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1



Verificación en dos pasos: protege las cuentas al generar un código de un solo uso que habrá que introducir en el proceso de login.

- **Google Authenticator:** disponible para su descarga en Google Play y Apple Store.
- **Microsoft Authenticator:** disponible para su descarga en Google Play y Apple Store.

VERIFICACIÓN EN 2 PASOS

La verificación en 2 pasos es una capa extra de protección para tus cuentas más sensiblres

Android:

- Accede a tu cuenta de Google > Seguridad > Verificación en dos pasos.
- Activa y selecciona método preferido: SMS, app (Google Authenticator), clave física.
- Opcional: agrega una segunda copia de seguridad.

iOS (Apple)

- Accede a tu cuenta de Google > Seguridad > Verificación en dos pasos.
- Activa y selecciona método preferido: SMS, app (Google Authenticator), clave física.
- Opcional: agrega una segunda copia de seguridad.

Consejo práctico:

- Usa apps como Google Authenticator, Microsoft Authenticator o Authy para mayor seguridad.
- Activa el doble factor al menos en correo, redes sociales, banca y gestor de contraseñas.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

ANTIRROBO

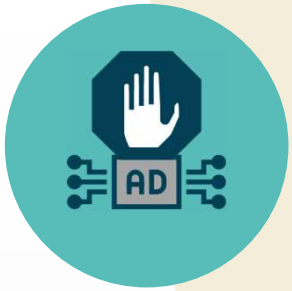
Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1



Antirrobo: ayuda a encontrar el dispositivo perdido o robado. Además, proporciona funciones como el borrado remoto de la información.

- **Encontrar mi dispositivo:** aplicación nativa para Android.
  - Ajustes > Google > Encontrar mi dispositivo

- **Buscar:** aplicación nativa para iOS.
  - Ajustes > Nombre de usuario > Buscar

ANTIRROBO

¿Y si pierdes o te roban el móvil? Las funciones antirrobo pueden ayudarte a localizarlo, bloquearlo o incluso borrar su contenido.

En Android:

- App nativa: "Encontrar mi dispositivo" Acceso: Ajustes > Google > Seguridad > Encontrar mi dispositivo

Permite hacer sonar, bloquear, mostrar mensaje, borrar datos remotamente.

En iOS:
App nativa: "Buscar"
Acceso: Ajustes > [Tu nombre] > Buscar > Buscar mi iPhone
Permite ver ubicación en el mapa, activar modo perdido, borrar contenido.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

CLAVES

- Activa siempre estas funciones desde el primer día.
- Asegúrate de tener la sesión iniciada con tu cuenta de Google o Apple.
- Un código de bloqueo y autenticación biométrica para evitar los accesos inmediatos.
- Estas herramientas no solo protegen el dispositivo, también protegen tu privacidad.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

DRAPER B1

COMPRAS SEGURAS

COMPRA SEGURA

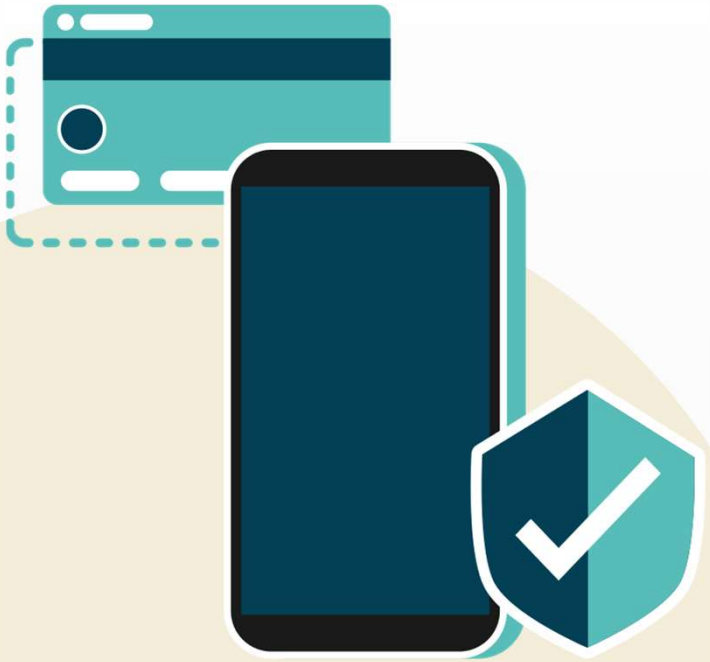
Hoy en día, el pago con los móviles se ha vuelto habitual Según un estudio de Visa y Mastercard, más del 30% de españoles utilizan sus smartphones para las compras. Pagar con el móvil es cómodo y rápido. La tecnología contactless ha simplificado este proceso, siendo aceptada en casi todos los establecimientos.

Compras seguras desde el móvil

- Asegúrate de que el sitio tenga HTTPS (candado al lado del link).
- Nunca ingreses datos bancarios en redes Wi-Fi abiertas. Usa tus datos o una red segura.
- Evita enlaces de mensajes sospechosos. Siempre accede directamente al sitio oficial.
- Usa apps oficiales: Amazon, MercadoLibre, no versiones modificadas.
- Activa notificaciones de tu banco para estar al tanto de compras.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

COMPRA SEGURA



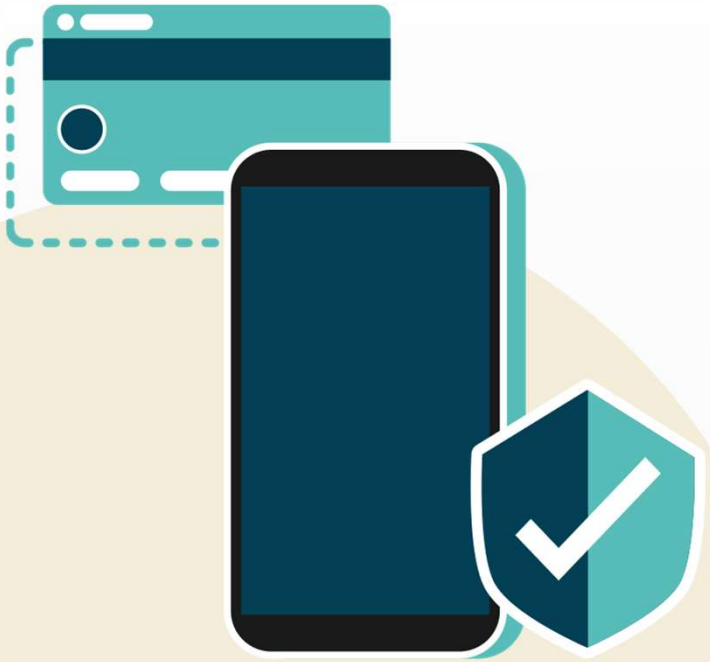
Pago Contactless y tarjetas monedero

- Activa el bloqueo de pantalla: sin él, cualquiera podría hacer pagos si pierde el teléfono.
- Desactiva el NFC cuando no lo estés usando para evitar lecturas indeseadas.
- Usa apps de pago oficiales como Google Wallet, Apple Pay o apps del banco.
- Revisa que la app de pagos tenga opciones de seguridad: PIN, huella, Face ID.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

COMPRA SEGURA

Tarjetas prepago, digitales y monederos virtuales:



- Son ideales para limitar riesgos: solo cargas lo necesario.
- Permiten separar tus compras online del saldo principal de tu banco.
- Muchos bancos permiten crear tarjetas virtuales temporales para una sola compra.
- Útiles en tiendas poco conocidas o para suscripciones de prueba.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

PREGUNTAS

- ¿ Qué es lo primero que vas a cambiar o revisar en tu móvil después de esta charla?
- ¿Tienes activada la verificación en dos pasos en tus cuentas principales?
- ¿Usas algún gestor de contraseñas o todavía memorizas las claves?
- ¿Revisas permisos de los apps que instalas?

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

MUCHAS GRACIAS

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
DRAPER B1

incibe_ emprende

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

DRAPER B1