

# Seguridad para dispositivos móviles, aplicaciones e Internet de las cosas

## Protección de datos y dispositivos en todo el mundo

Ante el aumento exponencial de los actores maliciosos en Internet y los ciberataques respaldados por gobiernos, creemos que nuestros productos y servicios deben ser tan seguros como útiles. En Google, nos esforzamos más que nunca para **proteger** a las personas, las organizaciones y los gobiernos compartiendo nuestro conocimiento especializado, **capacitando** a la sociedad para hacer frente a unos ciberriesgos en constante evolución y trabajando constantemente para **impulsar** avances en ciberseguridad que permitan construir **un mundo más seguro para todos**.

Por ello, asumimos el compromiso de mantenernos a la vanguardia y no dejar de mejorar nuestras soluciones de seguridad —en especial las dedicadas a proteger los dispositivos y aplicaciones conectados— para hacer frente a unas amenazas que aumentan constantemente y ofrecer a los usuarios un entorno seguro con múltiples opciones y control sobre los dispositivos que utilizan.

## El desafío

### La conectividad tiene un precio

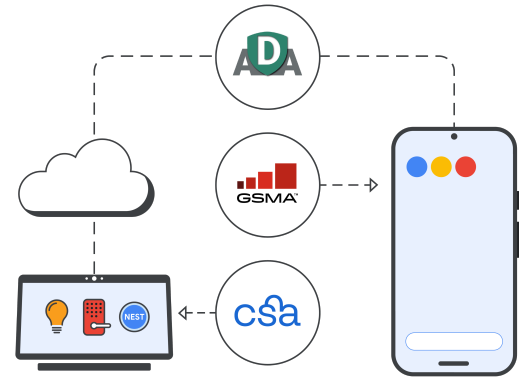
Gran parte de nuestra vida cotidiana se desarrolla en smartphones, aplicaciones y dispositivos de Internet de las cosas. Pasamos cada vez más tiempo en Internet y compartimos un número creciente de datos valiosos, como información bancaria o de salud. Por este motivo, estos dispositivos son más que nunca un objetivo prioritario de los ataques de ciberdelincuentes sofisticados que tratan de obtener información confidencial.

### Más dispositivos, más datos y más amenazas

Se calcula que en la actualidad hay en el mundo **17.000 millones de dispositivos de Internet de las cosas**. Estos incluyen desde impresoras hasta mecanismos de apertura de puertas de garaje, todos ellos con software (en algunos casos de código abierto) fácilmente pirateable.<sup>1</sup> El número total de dispositivos de Internet de las cosas vulnerados casi se **duplicó en 2020**.<sup>2</sup>

- ✓ Aunque estamos cada vez más conectados a través de dispositivos de Internet de las cosas, carecemos de normas globales que determinen el nivel de seguridad de estos productos, lo que impide a los usuarios tomar decisiones informadas sobre la seguridad de sus dispositivos.
- ✓ Igual que tienen derecho a conocer los ingredientes y componentes de los alimentos y productos de limpieza que compran, los consumidores deberían disfrutar de transparencia en los dispositivos y servicios digitales.
- ✓ Los dispositivos móviles son solo un vector más de otras muchas superficies de ataque, y la interconectividad de los dispositivos incrementa la necesidad de contar con información transparente a escala sobre su seguridad. Esto hace que la protección del ecosistema de dispositivos conectados sea tan importante como la de las redes y los sistemas.

## Colaboramos con organizaciones del sector



## Nuestra solución

En Google, ayudamos a mejorar la protección y transparencia de nuestros dispositivos conectados a través de soluciones de seguridad para dispositivos móviles, aplicaciones e Internet de las cosas:

### Seguridad para dispositivos móviles

Android, nuestro sistema operativo de código abierto, se basa en un enfoque de seguridad por capas para garantizar la protección de los dispositivos móviles:

- ✓ **Seguridad por capas**
  - El inicio verificado, la protección contra desinstalación de actualizaciones y la protección contra restablecimientos de fábrica garantizan el uso de la versión más reciente y segura de Android.
  - Las autenticaciones biométrica y por PIN protegen frente a accesos externos.
  - La función Encontrar Mi Dispositivo ayuda a localizar un dispositivo o a borrar los datos en caso de robo o pérdida.
- ✓ **Protección de identidades y contraseñas**
  - La verificación en dos pasos, la Llave de Seguridad integrada en el teléfono y el Gestor de Contraseñas protegen tu cuenta de Google frente a accesos externos.
  - La Revisión de Seguridad y la Protección Avanzada opcional permiten usar los dispositivos de forma segura e ininterrumpida.
- ✓ **Protección contra el phishing**
  - Las aplicaciones Teléfono de Google y Mensajes de Google ayudan a detectar y evitar estafas y ataques de phishing.
  - La Navegación Segura de Google protege a más de 5000 millones de dispositivos en todo el mundo.

### Seguridad para aplicaciones

La protección integrada contra software malicioso mantiene a raya las aplicaciones no seguras, y la información sobre seguridad de los datos ofrece transparencia a los usuarios cuando se descargan aplicaciones.

- ✓ **Google Play Store:** contamos con analistas humanos y herramientas de detección basadas en aprendizaje automático para revisar todas las aplicaciones antes de que los usuarios puedan descargarlas. La sección Seguridad de los datos explica qué tipo de datos recogen las aplicaciones y para qué se utilizan.
- ✓ **Google Play Protect:** analiza más de 125.000 millones de aplicaciones cada día y notifica, elimina o bloquea aquellas que plantean riesgos para la seguridad.
- ✓ **App Defense Alliance (ADA):** Google ha colaborado con partners líderes en detección de amenazas en dispositivos móviles para lanzar la App Defense Alliance, una iniciativa donde se comparte información y se coordinan medidas para proteger a los usuarios de Android de las aplicaciones potencialmente dañinas.

### Seguridad para el Internet de las cosas

Las etiquetas de seguridad para el Internet de las cosas indican de manera clara las prácticas de privacidad y seguridad que se aplican en un dispositivo, como los datos que este recoge.

- ✓ Aplicamos cinco principios fundamentales a los **programas de etiquetado de seguridad para el Internet de las cosas**: etiquetas en tiempo real, programas de evaluación, referencias de seguridad flexibles, transparencia de amplio espectro e incentivos de adopción.
- ✓ Colaboramos con la Connectivity Standards Alliance (**CSA**) y la GSM Alliance (**GSMA**) en la creación de un programa de certificación normalizado para toda la industria que cumpla las normativas actuales y futuras.

## Nuestros principios

En Google, aplicamos tres principios básicos para mejorar la seguridad y transparencia de nuestros dispositivos conectados:

**Defensa en profundidad:** empleamos una arquitectura de seguridad basada en diferentes capas que, combinadas, forman un sistema de defensa sólido que protege eficaz y correctamente.

**Apertura y transparencia:** la transparencia es un elemento clave de nuestra filosofía. Con la convicción de que un ecosistema de código abierto puede ser **más seguro** que uno cerrado, informamos a los usuarios de nuestra plataforma y compartimos conocimientos para mejorar nuestra protección.

**Los mejores de Google y del ecosistema:** colaboramos con equipos de expertos de Google y de la industria para ayudar a proteger a miles de millones de usuarios.

## Aplicaciones

### Etiquetas de seguridad para el Internet de las cosas: el control en manos de los consumidores

Sin un etiquetado estandarizado para la seguridad del Internet de las cosas, los fabricantes de dispositivos carecen de normas internacionales que puedan usar como referencia. Por otro lado, los usuarios no tienen toda la información que deberían para saber si sus dispositivos protegen sus datos. La industria debe aunar esfuerzos para impulsar la seguridad del Internet de las cosas y devolver el control a los consumidores. A través de nuestros procesos y colaboraciones, estamos trabajando en la creación de un programa de etiquetado de seguridad para el Internet de las cosas.

En primer lugar, invertimos en [investigaciones externas en seguridad](#) para detectar posibles vulnerabilidades (Google Nest participa en el [programa Vulnerability Reward](#)) y ofrece recompensas a los aficionados y profesionales de la seguridad ajenos a Google que detectan vulnerabilidades).

Gracias a estas, publicamos parches y correcciones de errores críticos durante un mínimo de cinco años tras el lanzamiento del producto.

Todos los dispositivos que hemos desarrollado a partir de 2019 incorporan el [inicio verificado](#) para garantizar la ejecución del software adecuado y la protección del acceso. Por ejemplo, nuestros [dispositivos Google Nest](#) se validan a partir de normas de seguridad de terceros reconocidas por el sector, como las desarrolladas por el ETSI y la ISO.

Estas normas, junto con nuestro ciclo seguro de vida del desarrollo de software (SDLC), reducen la probabilidad de que los consumidores se vean expuestos a malas prácticas de seguridad y allanan el camino hacia un Internet abierto y más seguro.

## Nuestros logros e inversiones en el sector



## Nuestro enfoque

### Comprometidos con un mundo digital abierto y seguro

Con el aumento del volumen de datos en un número creciente de dispositivos en distintas redes, la preocupación por la seguridad no hará sino aumentar. En Google, contribuimos a impulsar el futuro de la protección de los dispositivos conectados mediante el desarrollo de productos, criterios de transparencia y colaboraciones con organizaciones del sector.

Uno de los pilares clave de nuestra estrategia de producto es garantizar la seguridad predeterminada de los mismos. La Navegación Segura, Google Play Protect y la Llave de Seguridad integrada protegen los dispositivos y aplicaciones móviles para ofrecer el máximo nivel de seguridad.

Al abordar los problemas de forma abierta y transparente, y compartir nuestros conocimientos sobre protección de los dispositivos conectados, ayudamos a democratizar las operaciones de seguridad. Nuestro enfoque de seguridad por capas se basa en la convicción de que un ecosistema de código abierto puede ser más seguro que uno cerrado.

Nuestras colaboraciones con la CSA, la ADA y la GSMA reflejan nuestros esfuerzos por impulsar avances en ciberseguridad que permitan construir un Internet y un futuro más seguros para todos.



Tenemos el compromiso de mejorar el nivel de seguridad de los dispositivos conectados y sentar las bases para que Internet sea un entorno más seguro para todos los usuarios en todas partes. Puedes obtener más información sobre los avances de Google en materia de seguridad de los dispositivos conectados en: [g.co/connecteddevicesafety](https://g.co/connecteddevicesafety)