



Nuestra trayectoria en ciberseguridad a lo largo de los años

Más seguridad con Google

Mantenemos a más personas seguras en línea que nadie en el mundo

Considerando el incremento radical de los ciberataques patrocinados por gobiernos y actores maliciosos en línea, creemos que nuestros productos y servicios son tan útiles como seguros.

En Google, estamos más enfocados que nunca en **proteger** a las personas, las organizaciones y los gobiernos con nuestra experiencia: **capacitamos** a la sociedad para combatir los riesgos cibernéticos en constante evolución y trabajamos continuamente para **progresar** en el arte de la ciberseguridad para construir **un mundo más seguro para todas las personas**.



Innovamos continuamente a través de los años

Desde el lanzamiento de Gmail en 2004 hasta la incorporación de la Computación protegida en 2022, Google ha sido pionero en tecnología de ciberseguridad y ha innovado continuamente en productos, plataformas y asociaciones para eliminar todo tipo de amenazas con el fin de crear un futuro más seguro para las personas, las organizaciones y la sociedad:

- ✓ Desarrollamos productos y plataformas seguras
- ✓ Creamos equipos de seguridad ágiles
- ✓ Fomentamos programas y alianzas
- ✓ Ofrecemos financiación crítica para la innovación y la formación de personal

A medida que evolucionan las necesidades de las personas e internet, seguimos a la vanguardia de las nuevas tecnologías para mitigar las ciberamenazas en constante cambio y garantizamos que cada día sea más seguro con Google.

2004
Protección contra el spam en Gmail

Fuimos uno de los primeros en crear protecciones para correo electrónico basadas en inteligencia artificial.

🔗 Gmail **bloquea** ▲ el **99.9%** de los correos electrónicos peligrosos y sospechosos.

2007
Navegación segura

Protegemos de forma proactiva los dispositivos de todo el mundo al alertar a los/las usuarios/as cuando visitan sitios web peligrosos. En 2020, la protección en línea evolucionó hacia la **Navegación segura mejorada**.

👤 **5,000 millones** de dispositivos **protegidos** ♥ por la Navegación segura

2009
reCAPTCHA

Adquirimos la solución de gestión de fraudes y bots para detener el relleno de credenciales y la apropiación de cuentas, y para evitar actividades abusivas de software malicioso/usuarios falsos.

▲ **5 millones** de sitios web **defendidos** ♥

2008
Administrador de contraseñas de Google

Al incorporar el Administrador de contraseñas, logramos que el inicio de sesión fuera más fácil y seguro, sin necesidad de recordar o escribir las contraseñas. Hoy en día, se utiliza para el 50% de todos los inicios de sesión en Chrome en todas las plataformas.

🔑 **1,000 millones** de contraseñas **verificadas** ♥ diariamente en busca de vulneraciones

2010
Zero Trust

Después de sobrevivir a la Operación Aurora (una serie coordinada de **ciberataques**), revolucionamos nuestro enfoque para construir una arquitectura segura por diseño que ahora se conoce como Zero Trust (confianza cero). Garantiza menos segmentos de ataque, menos oportunidades de perder datos y más control sobre los sistemas de los que dependen los usuarios. Apoyamos las iniciativas de la Casa Blanca para desplegar el modelo Zero Trust en todo el gobierno federal y también lo empaquetamos en BeyondCorp Enterprise para que cualquier empresa pueda aprovecharlo.

2010
Grupo de análisis de amenazas (TAG)

Tras la Operación Aurora, formamos un equipo especializado de expertos **responsables** en detectar, analizar y desmantelar las ciberamenazas hacia el gobierno y las ciberamenazas delictivas graves. TAG localizó en Corea del Norte el origen de Wanna Cry, el mayor ataque de ransomware de la historia, y recientemente compartió **ejemplos** de los ecosistemas de hackeo por encargo de India, Rusia y Emiratos Árabes Unidos.

2010
Google Bug Hunters

A muchos estudiantes de preparatoria, abogados, profesionales de TI y aficionados a la caza de errores en los productos de Google les atrae nuestro programa Vulnerability Rewards, ya que hay premios en efectivo. Sus motivos varían, pero su misión es la misma: encontrar vulnerabilidades no descubiertas para mantener la seguridad de los servicios en línea.

💰 **Millones** de dólares pagados en recompensas desde 2010

2010
The Red Team (El equipo rojo)

Fue creado para adoptar la mentalidad de nuestros adversarios y hackear a Google para reforzar nuestras defensas y detectar lagunas. Trabajan en todo el mundo para mantenerse al día de las amenazas más recientes, mejorar los controles de seguridad, llevar a cabo la detección/prevenición de ataques y eliminar todo tipo de vulnerabilidades al impulsar marcos de trabajo nuevos y mejores.

2013
Project Shield

Project Shield identifica amenazas, aplica la ley y habilita respuestas en la comunidad de seguridad con el fin de proteger las noticias, organizaciones de derechos humanos, sitios electorales, organizaciones políticas y campañas de ataques de denegación de servicio (DDoS) en más de 100 países.

🌐 **Más de 150** sitios web **actualmente protegidos** ♥ en Ucrania

2011
Verificación en dos pasos

Fuimos uno de los primeros (2SV) por defecto y los primeros en activar automáticamente 2SV para más de 150 millones de personas en 2021, para ofrecer una forma segura y fácil de iniciar sesión. Incluso si te roban la contraseña, tu cuenta está protegida.

🔒 **Disminución del 50%** de cuentas afectadas desde la 2SV

2014
Project Zero

Un grupo de trabajo especializado dedicado a la caza de exploits de día cero en internet (en software, hardware, productos de Google, etc.) para garantizar un internet seguro y abierto. Fueron los primeros en dar detalles sobre "Melttdown" y "Specter", lo que permitió a los desarrolladores abordar rápidamente las vulnerabilidades de CPU y aplicar mitigaciones en toda la cadena de suministro de software.

2017
Programa de protección avanzada (APP)

Protecciones extra seguras (por ejemplo, la Llave de seguridad) para usuarios de alta visibilidad y alto riesgo como periodistas y funcionarios del gobierno.

👤 **Más de 300** campañas federales **protegidas** ♥

2018
Llave de seguridad Titan

Creamos la Llave de seguridad Titan para los usuarios que buscan una solución integral en Google. Las llaves cumplen con el estándar FIDO y también se pueden utilizar en otros lugares, no solo con Google.

2017
Google Play Protect

Google Play Protect es el servicio de protección frente a amenazas móviles más implementado en el mundo. Siempre está en constante adaptación y mejora gracias al aprendizaje automático de Google para analizar automáticamente las aplicaciones en busca de malware y cifrar los pagos de los usuarios en teléfonos Android.

🔍 **Más de 100,000 millones** de aplicaciones analizadas diariamente en busca de malware

🔒 **150 millones** de pagos de usuarios **cifrados** ♥ diariamente

2019
Reautenticación sin contraseña

Ampliamos nuestra compatibilidad con FIDO en Android para que los usuarios puedan iniciar sesión sin problemas en sitios web con solo un PIN o autenticación biométrica, sin necesidad de contraseña.

2021
Inversión para avanzar en ciberseguridad

Nos comprometemos a reforzar la ciberseguridad, ampliar los programas de confianza cero, ayudar a proteger la cadena de suministro de software y mejorar la seguridad del código abierto. Buscamos formar a 100,000 estadounidenses en campos como el soporte informático y el análisis de datos a través del programa de Certificados de Carrera de Google.

💰 **10,000 millones de USD** destinados para iniciativas de ciberseguridad

2021
Computación confidencial

Para la seguridad, protección y privacidad críticas, presentamos Google Cloud Confidential Computing, una tecnología innovadora que mantiene los datos cifrados mientras son procesados, lo que permite que permanezcan seguros durante todo su ciclo de vida, incluso mientras están en reposo o en tránsito. Ahora, incluso los datos más confidenciales pueden migrarse a la nube con total confianza.

2021
Equipo de seguridad de código abierto de Google (GOSST)

GOSST se creó para mejorar la seguridad del software de código abierto en el que confía el mundo. Nos asociamos con la Fundación de Seguridad del Código Abierto (OpenSSF) para desarrollar y publicar Supply-Chain Levels for Software Artifacts (SLSA), un marco para proteger la cadena de suministro de software y permitir la seguridad a largo plazo en todo el ecosistema de software.

💰 **100 millones de USD** destinados a operaciones de seguridad de código abierto de terceros para solucionar vulnerabilidades.

2022
Estandarización de la criptografía poscuántica

Siempre pensamos a futuro y seguimos desarrollando sistemas criptográficos de nueva generación para combatir la ruptura de los criptosistemas de clave pública y las comunicaciones digitales en peligro. El Instituto Nacional de Estándares y Tecnología seleccionó una propuesta en la que participó Google (SPHINCS+) para llevar a cabo la estandarización.

2022
Computación protegida

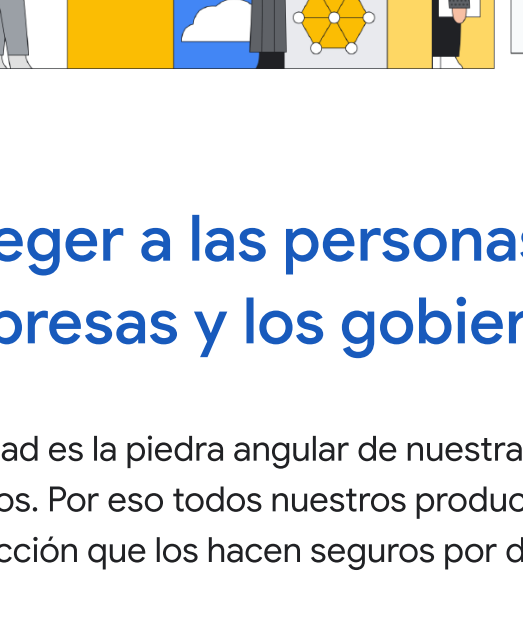
Anunciamos la Computación Protegida, un conjunto creciente de tecnologías que transforma cómo, cuándo y dónde se procesan los datos para garantizar de forma técnica la privacidad y la seguridad del usuario. Lo hacemos minimizando la huella de los datos, desidentificándolos y restringiendo el acceso a los datos sensibles. Esto significa que Android puede sugerir la siguiente frase en un texto y mantener completamente la privacidad de la conversación.

2023
Llave de acceso: un futuro sin contraseñas

Llevamos más de una década preparando el terreno para un futuro sin contraseñas. Nos unimos a la Alianza FIDO en 2013 para impulsar estándares abiertos para un mundo sin contraseñas y ahora, al ampliar nuestro soporte para los estándares de inicio de sesión FIDO a Android y Chrome a través de la tecnología Llave de acceso en 2023, finalmente tendremos la plataforma para un futuro en el que de verdad no haya contraseñas.

2022
Mandiant y Google Cloud

Mandiant aporta información exhaustiva y en tiempo real sobre amenazas que obtiene de la primera línea de ciberseguridad de las mayores organizaciones del mundo. En combinación con las ofertas de seguridad nativa en la nube de Google Cloud, ayudamos a las empresas y a los organismos del sector público a mantenerse protegidos durante todo el ciclo de vida de la seguridad.



En una era en la que el alcance tecnológico es cada vez mayor, la confianza en la tecnología es clave para liberar el verdadero potencial de la sociedad.

A medida que pongamos en práctica nuestros conocimientos sobre seguridad, seguiremos colaborando con personas, empresas y gobiernos para proteger su seguridad e impulsar una nueva era en ciberseguridad.



Proteger a las personas, las empresas y los gobiernos

La seguridad es la piedra angular de nuestra estrategia de productos. Por eso todos nuestros productos ofrecen protección que los hacen seguros por diseño.

Empoderamos a la sociedad para hacer frente a los riesgos cambiantes de la ciberseguridad

Empoderamos a las sociedades para liberar el potencial del código abierto y compartimos nuestros conocimientos y experiencia de forma transparente con la industria para mantener los ecosistemas más seguros.



Anticipamos las tecnologías del futuro

Queremos proteger a las sociedades de la próxima generación de ciberamenazas. Nos basamos en nuestra experiencia en IA para diseñar la próxima generación de arquitecturas para ampliar los límites de la innovación en seguridad.

Cada día es más seguro con Google

Visita [g.co/safety/cyber](https://www.google.com/safety/cyber)

