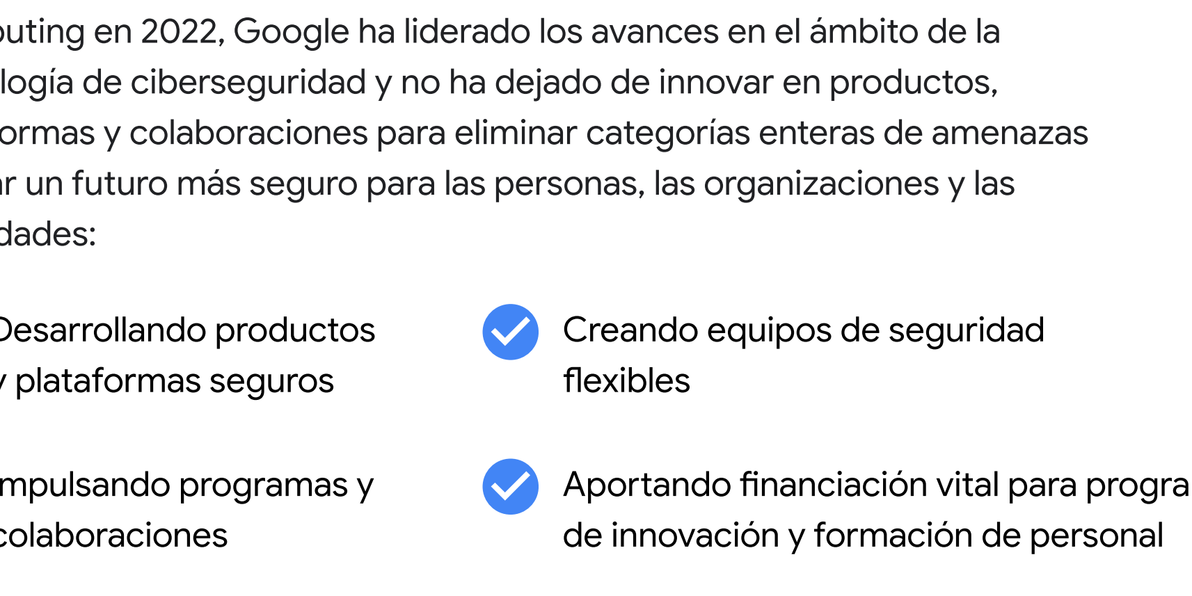
Nuestro viaje por la ciberseguridad a lo largo de los años

Más seguridad con Google

Google trabaja cada día para hacer que Internet sea más seguro para todos

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.



Innovación año tras año

Desde el lanzamiento de Gmail en 2004 hasta la presentación de Protected Computing en 2022, Google ha liderado los avances en el ámbito de la tecnología de ciberseguridad y no ha dejado de innovar en productos, plataformas y colaboraciones para eliminar categorías enteras de amenazas y crear un futuro más seguro para las personas, las organizaciones y las sociedades:

- ✓ Desarrollando productos y plataformas seguros
- ✓ Creando equipos de seguridad flexibles
- ✓ Impulsando programas y colaboraciones
- ✓ Aportando financiación vital para programas de innovación y formación de personal

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

2004
Gmail incluye la protección contra spam

Fuimos una de las primeras organizaciones en crear herramientas de protección de correo electrónico basadas en IA.

Gmail bloquea el 99,9 % de los correos electrónicos peligrosos y sospechosos

2007
Navegación Segura

Alertamos a los usuarios que visitan sitios web peligrosos para proteger proactivamente los dispositivos en todo el mundo, una protección online que en 2020 se convirtió en la Navegación Segura Mejorada.

La Navegación Segura protege más de 5000 millones de dispositivos en todo el mundo.

2008
Gestor de Contraseñas de Google

Con la introducción del Gestor de Contraseñas, que evita tener que recordar o escribir las contraseñas, conseguimos que iniciar sesión fuera más fácil y seguro. Ahora, esta función se utiliza en el 50 % de todos los inicios de sesión en Chrome en todas las plataformas.

Cada día, se verifican 1000 millones de contraseñas para comprobar que no han sido vulneradas

2009
reCAPTCHA

Adquirimos esta solución de bots antifraude para poner freno a la reutilización de credenciales y la apropiación de cuentas, así como para impedir las actividades abusivas perpetradas por software malicioso/falsos usuarios.

Se protegen 5 millones de sitios web

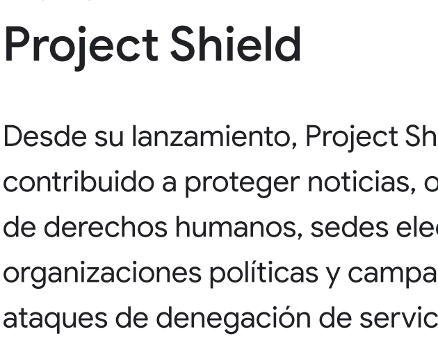
2010
Confianza cero

Tras sobrevivir a la Operación Aurora, una serie de ciberataques coordinados, transformamos nuestra estrategia para desarrollar un modelo de protección intrínsecamente seguro que actualmente se conoce como "confianza cero". Esta estrategia reduce el número de vectores de ataque y la posibilidad de perder datos y proporciona más control sobre los sistemas de los que dependen los usuarios. Además de apoyar los esfuerzos del Gobierno de EE. UU. para implementar el modelo de confianza cero en todas sus redes y sistemas, lo hemos integrado en nuestra solución BeyondCorp Enterprise para que cualquier empresa pueda beneficiarse de él.

2010
Grupo de Análisis de Amenazas (TAG)

Tras la Operación Aurora, creamos un equipo especializado de expertos al que asignamos la tarea de detectar, analizar y desarticular ciberamenazas graves de grupos delictivos o patrocinadas por gobiernos. Después de identificar el origen de Wanna Cry, el mayor ataque de ransomware de la historia, en Corea del Norte, el TAG ha compartido recientemente pruebas de la existencia de ecosistemas de piratas informáticos a sueldo en India, Rusia y Emiratos Árabes Unidos.

2010
Bug Hunters de Google



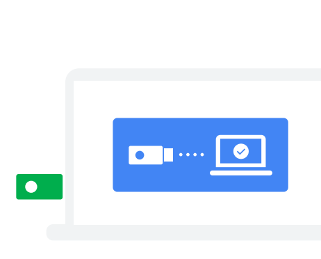
Nuestro programa Vulnerability Reward atrae a estudiantes universitarios, profesionales del derecho y la TI y aficionados a la seguridad y les ofrece recompensas en metálico por detectar errores en los productos de Google. Aunque sus motivaciones varían, su misión es siempre la misma: detectar vulnerabilidades no descubiertas para garantizar la seguridad de los servicios en Internet.

Desde 2010, Google ha repartido millones de dólares en recompensas

2010
El Red Team

Creamos el Red Team con el objetivo de ponernos en el lugar de nuestros adversarios e intentar piratear nuestros sistemas para reforzar nuestras defensas y detectar sus puntos débiles. Sus miembros trabajan en todo el mundo para crear nuevos marcos más eficientes, manteniéndose al día de las amenazas más recientes, mejorando los controles de seguridad, detectando/previniendo ataques y eliminando categorías enteras de vulnerabilidades.

2011
Verificación en dos pasos



Fuimos una de las primeras organizaciones en integrar un sistema predeterminado de verificación en dos pasos en nuestros productos, y la primera en habilitarla automáticamente en las cuentas de más de 150 millones de usuarios en 2021 para ofrecerles una forma segura y fácil de iniciar sesión. Así, sus cuentas siguen estando protegidas aunque les roben la contraseña.

Desde la introducción de la verificación en dos pasos, la vulneración de cuentas se ha reducido en un 50 %

2013
Project Shield

Desde su lanzamiento, Project Shield ha contribuido a proteger noticias, organizaciones de derechos humanos, sedes electorales, organizaciones políticas y campañas frente a ataques de denegación de servicio distribuido (DDoS) y otros ciberataques en más de 100 países identificando amenazas y facilitando la respuesta de la comunidad de seguridad y los cuerpos policiales.

Actualmente, Project Shield protege más de 150 sitios web en Ucrania

2014
Project Zero

Este grupo de trabajo especializado se dedica en exclusiva a detectar vulnerabilidades de día cero en Internet, analizando software, hardware, productos de Google y otros elementos para garantizar un Internet seguro y abierto. Sus integrantes fueron los primeros en descifrar los fallos de seguridad "Meltdown" y "Spectre", lo que permitió a los desarrolladores abordar rápidamente las vulnerabilidades de las CPU afectadas y aplicar medidas de mitigación en toda la cadena de suministro del software.

2017
Programa de Protección Avanzada

Con este programa introdujimos medidas de protección adicionales, entre ellas la Llave de seguridad, para usuarios de alta visibilidad y alto riesgo como periodistas y funcionarios gubernamentales.

El Programa de Protección Avanzada protege más de 300 campañas del Gobierno federal

2017
Google Play Protect

Google Play Protect, el servicio de protección frente a amenazas en dispositivos móviles más utilizado del mundo, que se adapta y mejora constantemente gracias al aprendizaje automático de Google, analiza automáticamente las aplicaciones en busca de software malicioso y cifra los pagos de los usuarios en teléfonos Android.

Cada día se analizan más de 100.000 millones de aplicaciones en busca de software malicioso

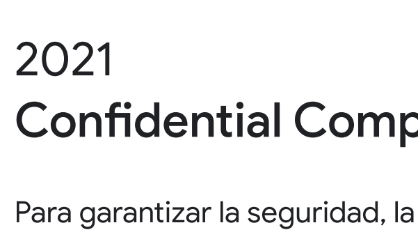
Cada día Google Play Protect cifra 150 millones de pagos de usuarios

2018
Llave de seguridad Titan

Creamos la Llave de seguridad Titan para los usuarios que demandaban una solución integral de Google. Las llaves cumplen las normas de la FIDO y también pueden utilizarse fuera de Google.

2019
Reautenticación sin contraseña

Ampliamos la compatibilidad de Android con las normas de la FIDO para que los usuarios pudieran iniciar sesión en sitios web sin interrupciones ni contraseñas utilizando solo un PIN o datos biométricos.



2019
Chronicle

Introdujimos Chronicle, una capa especializada adicional que complementa nuestra infraestructura básica, para proporcionar a las empresas una solución de seguridad privada basada en la nube con la que almacenar, analizar y buscar grandes volúmenes de datos de redes y seguridad.

2021
Inversiones para impulsar la ciberseguridad

Adquirimos el compromiso de reforzar la ciberseguridad, ampliar los programas de confianza cero, ayudar a proteger la cadena de suministro del software y mejorar la seguridad del código abierto. Nos comprometimos a formar a 100.000 estadounidenses en campos como el soporte de TI y el análisis de datos a través del programa de Certificados Profesionales de Google.

Google se ha comprometido a invertir 10.000 millones de dólares en iniciativas de ciberseguridad

2021
Confidential Computing

Para garantizar la seguridad, la protección y la privacidad de los datos críticos, introdujimos Confidential Computing de Google Cloud, una tecnología innovadora que cifra los datos mientras se procesan para que permanezcan protegidos durante todo su ciclo de vida, incluso mientras están en reposo o en tránsito. Ahora, hasta los datos más sensibles pueden migrarse a la nube con total confianza.

2021
Equipo de Seguridad del Código Abierto de Google

El Equipo de Seguridad del Código Abierto de Google nació con la finalidad de mejorar la seguridad del software de código abierto que se utiliza en todo el mundo. Colaboramos con la Open Source Security Foundation (OpenSSF) para desarrollar y publicar el SLSA (Supply-Chain Levels for Software Artifacts), un marco que protege la cadena de suministro del software y garantiza la seguridad a largo plazo en todo su ecosistema.

Google se ha comprometido a destinar 100 millones de dólares a actividades de seguridad de otras organizaciones para corregir vulnerabilidades en el código abierto

2022
Normalización de la criptografía poscuántica

Con la vista puesta en el futuro, seguimos desarrollando sistemas criptográficos de nueva generación que protegen frente a las vulneraciones de los criptosistemas de clave pública y las comunicaciones digitales. Recientemente, el National Institute of Standards and Technology seleccionó el SPHINCS+, un modelo en cuyo desarrollo ha participado Google, para su normalización.

2022
Protected Computing

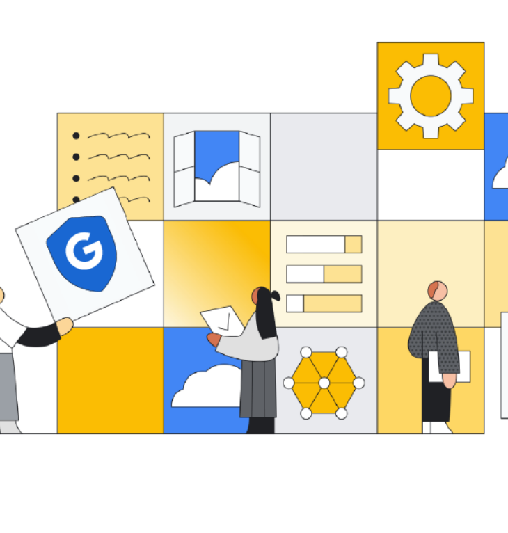
Anunciamos Protected Computing, un kit de recursos técnicos que se amplía continuamente y que transforma cómo, cuándo y dónde se tratan los datos para garantizar su privacidad y seguridad mediante soluciones tecnológicas. Para conseguirlo, minimizamos la huella de datos, desidentificamos la información y restringimos el acceso a los datos sensibles. Gracias a Protected Computing, Android puede sugerir a un usuario la siguiente frase del texto que está escribiendo mientras garantiza la total privacidad de su conversación.

2022
Mandiant y Google Cloud

Mandiant ofrece en tiempo real información detallada de primera línea sobre ciberseguridad y la comparte con las mayores organizaciones del planeta. Combinada con la oferta de seguridad nativa de la nube de Google Cloud, esta información ayuda a empresas y organismos públicos a protegerse en todo el ciclo de vida de la seguridad.

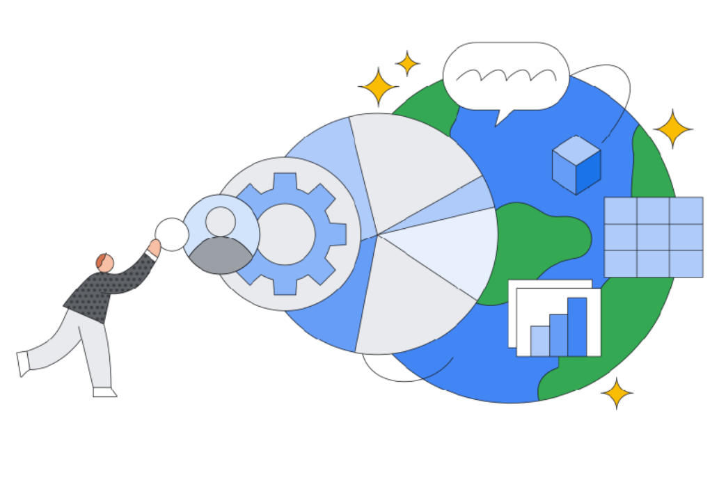
2023
Las llaves de acceso abren la puerta a un futuro sin contraseñas

Llevamos más de una década allanando el camino para un futuro sin contraseñas. En 2013, ingresamos en la FIDO Alliance para impulsar el desarrollo de normas abiertas para un mundo sin contraseñas. En 2023, hemos ampliado la compatibilidad de Android y Chrome con las normas de inicio de sesión de la organización mediante la tecnología de llaves de acceso para, por fin, crear una plataforma que permita un futuro sin contraseñas.



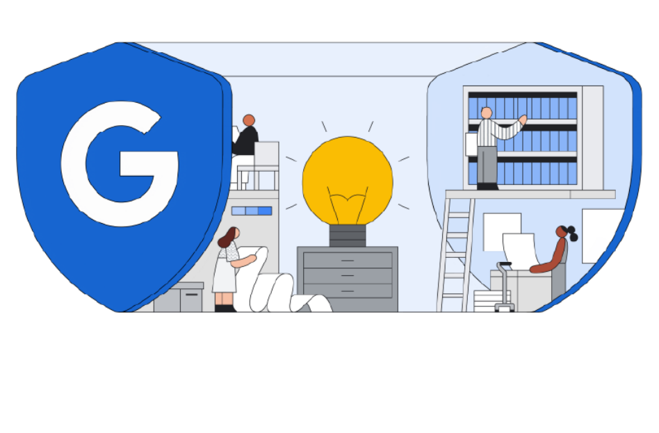
En una época en la que el alcance de la tecnología es cada vez mayor, la confianza en ella es clave para que la sociedad desarrolle su verdadero potencial.

Mientras ponemos en práctica nuestros conocimientos de seguridad, seguiremos colaborando con personas, empresas y gobiernos para protegerlos e impulsar el comienzo de una nueva era en la ciberseguridad.



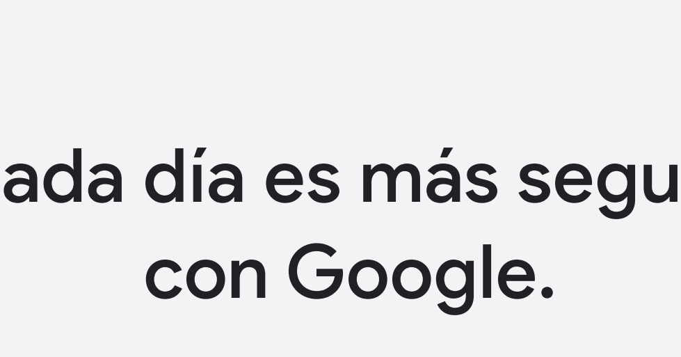
Proteger a las personas, las empresas y los gobiernos

La seguridad es la pieza clave de nuestra estrategia. Por este motivo, todos nuestros productos incorporan medidas de protección que los hacen intrínsecamente seguros.



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

Capacitamos a las sociedades para que puedan explotar todo el potencial que ofrece el código abierto y compartimos transparentemente nuestro conocimiento especializado y experiencia en el sector para mejorar la protección de los ecosistemas.



Impulsar las tecnologías del futuro

Nuestro objetivo es proteger a las sociedades frente a la próxima generación de ciberamenazas. Partiendo de nuestro conocimiento especializado de la IA, estamos diseñando una nueva generación de arquitecturas que trascenderá los límites de la innovación en seguridad.

Cada día es más seguro con Google.

Visita g.co/safety/cyber