chrome enterprise

Reduce los riesgos de quiebra de seguridad de datos y robo de identidad en la empresa con Alerta de Protección de Contraseña del navegador Chrome

Introducción

¿Hasta qué punto pueden estar protegidos tus datos y tu organización si un elevado porcentaje de empleados reutiliza su contraseña de trabajo en otros sitios?

En una encuesta realizada por Google y Harris Poll en el 2019, preguntaron a 3000 adultos si reutilizaban su contraseña y el 65 % respondió que lo hacía en varias cuentas, aunque no en todas, o que usaba exactamente la misma contraseña *en todas sus cuentas*.

Reutilizar la contraseña sigue siendo una práctica habitual

52 % Usa la misma contraseña en varias cuentas, aunque no en todas

35 % Usa una contraseña distinta en cada cuenta

13 % Usa la misma contraseña en todas sus cuentas

chrome enterprise

Por lo tanto, a un hacker le basta con piratear *la contraseña del trabajo de un empleado* para obtener acceso a los dispositivos de esa persona y a la red y los datos de su empresa. Los piratas informáticos emplean muchos métodos para conseguir las contraseñas, pero los tres más comunes son los ataques de fuerza bruta para adivinarlas, la ingeniería social y el phishing.

¿Y si el navegador Chrome impidiese de forma proactiva que se reutilizara la contraseña del trabajo?
Tu organización y sus empleados contarían con una capa más de protección, y tú disfrutarías de más tranquilidad.

Política Alerta de Protección de Contraseña del navegador Chrome

Alerta de Protección de Contraseña del navegador Chrome es una política que permite a las empresas evitar el robo de identidad y la quiebra de seguridad de datos de los empleados y la organización detectando si algún empleado introduce sus credenciales de trabajo en otro sitio web.

La política Alerta de Protección de Contraseña del navegador Chrome amplía esa capacidad y refuerza la seguridad de las cuentas y los datos de las empresas protegiendo las credenciales de Google *y también* las que no son de Google. Permite que el departamento de TI gestione las directrices de esta política en todos los sistemas operativos más importantes, como ChromeOS, Windows[1], Mac[2] y Linux.

Protección de la privacidad

En Google nos tomamos muy en serio la privacidad de los usuarios. Solo almacenamos en el disco una huella digital no reversible de las contraseñas. Nadie puede ver las credenciales de los usuarios. **Los datos de las credenciales no salen nunca del equipo local. Nunca se envían a Google ni se comparten con terceros.** No te preocupes: activar Alerta de Protección de Contraseña no pone en peligro la privacidad ni la seguridad de los usuarios.

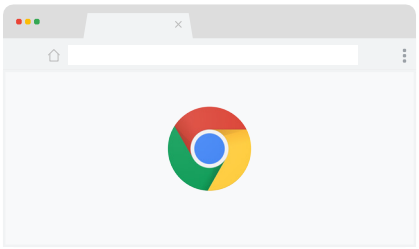
[1] Microsoft®, Windows® e Internet Explorer® son marcas registradas de Microsoft Corporation en Estados Unidos u otros países.

[2] Mac y macOS son marcas de Apple Inc. registradas en Estados Unidos y otros países.

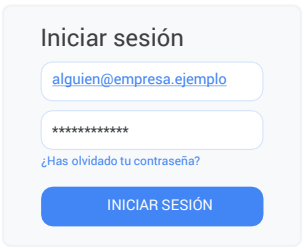
chrome enterprise

Cómo funciona Alerta de Protección de Contraseña

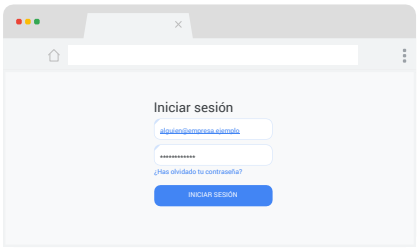
En primer lugar, fijémonos en Alerta de Protección de Contraseña desde el punto de vista del usuario final. Después de que el departamento de TI habilite esta política, el usuario disfruta de una experiencia fluida.



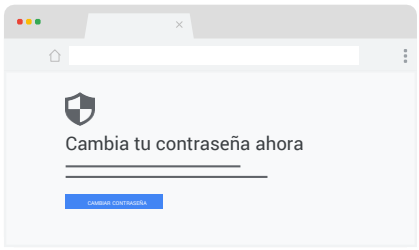
1. El usuario abre el navegador Chrome.



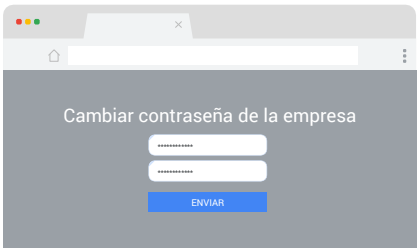
2. Inicia sesión en la red de la empresa con sus credenciales habituales.



3. Va a un sitio y usa la misma contraseña, aunque cambie el nombre de usuario.



4. Alerta de Protección de Contraseña avisa al usuario de que está utilizando la misma contraseña. El usuario tiene una opción:



5. Ir a la página para cambiar su contraseña.

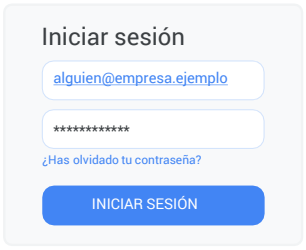
Cuando un usuario emplea sus credenciales de trabajo en un sitio web que no pertenece a la empresa, se le muestra una advertencia y se le dirige a la página para cambiar su contraseña por si quiere hacerlo.

Y esto es lo que sucede en el backend cuando se habilita Alerta de Protección de Contraseña:

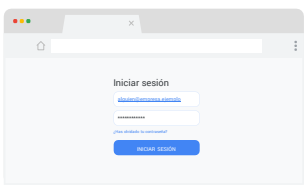
1. El usuario inicia sesión en la red de la empresa con sus credenciales habituales.

2. Sin preguntar nada al usuario, que no sabe qué pasa en el backend, Alerta de Protección de Contraseña captura la contraseña y la almacena en forma de hash en el equipo local.

3. El usuario sigue trabajando como si nada.



1



3

Puedes configurar Alerta de Protección de Contraseña para que funcione de dos modos.

El modo de **monitorización pasiva** registra cada vez que se reutiliza una contraseña en el sistema de archivos local o el registro de eventos de Windows sin mostrar ninguna advertencia al usuario final. Así obtienes información sobre la incidencia de esta práctica en tu empresa.

El modo de **detección activa** muestra una advertencia al usuario cuando introduce sus credenciales de trabajo en sitios web ajenos a la empresa o de phishing. Estos casos también se pueden registrar en el sistema de archivos local o el registro de eventos de Windows.

chrome enterprise

Cómo habilitar Alerta de Protección de Contraseña

La política Alerta de Protección de Contraseña está incluida en las plantillas de Enterprise de Google. En todos los sistemas operativos, puedes habilitar Alerta de Protección de Contraseña en la consola de Gestión en la nube del navegador Chrome. En los entornos de Microsoft, también puedes hacerlo mediante una directiva de grupo.

Cómo usar Alerta de Protección de Contraseña del navegador Chrome

Configurar Alerta de Protección de Contraseña resulta muy sencillo para los clientes de G Suite, para los clientes de G Suite con SSO y para los clientes que no usan G Suite. La política Alerta de Protección de Contraseña se puede habilitar en cualquier navegador Chrome Enterprise que se gestione mediante objetos de directivas de grupo o la nube. Tienes a tu disposición más información sobre cómo gestionar el navegador Chrome Enterprise en la nube o mediante directivas de grupo. Lee también el informe técnico sobre Alerta de Protección de Contraseña del navegador Chrome para aprender a configurar paso a paso esta política según las distintas opciones.

Conclusión

Alerta de Protección de Contraseña del navegador Chrome añade otra capa más de protección a tu empresa, ya que muestra una advertencia a los usuarios cuando intentan reutilizar su contraseña del trabajo en sitios web de phishing o sitios no aprobados. En un mundo tan hiperconectado como el actual, donde el phishing y otros tipos de ataques están a la orden del día y causan estragos, Alerta de Protección de Contraseña es una herramienta imprescindible de tu conjunto de seguridad empresarial.

Por último, si quieres conocer más a fondo Alerta de Protección de Contraseña del navegador Chrome, **consulta estos recursos:**

Vídeo sobre la política Alerta de Protección de Contraseña

Más información sobre Alerta de Protección de Contraseña del navegador Chrome

Ayuda para administradores de G Suite: Preguntas frecuentes sobre la extensión Alerta de Protección de Contraseña para prevenir la suplantación de identidad (phishing)

Más información sobre cómo evitar que los usuarios reciban ataques de phishing

Descargar el navegador Chrome para tu empresa

Más información sobre Asistencia para empresas del navegador Chrome

Lista de políticas del navegador Chrome

Notas de la versión del navegador Chrome para empresas

Novedades y actualizaciones del navegador Chrome en el blog sobre versiones de Chrome

Blog oficial de Google sobre seguridad

Centro de Ayuda de Chrome Enterprise y foro de ayuda del navegador Chrome

Registro público de errores del navegador Chrome