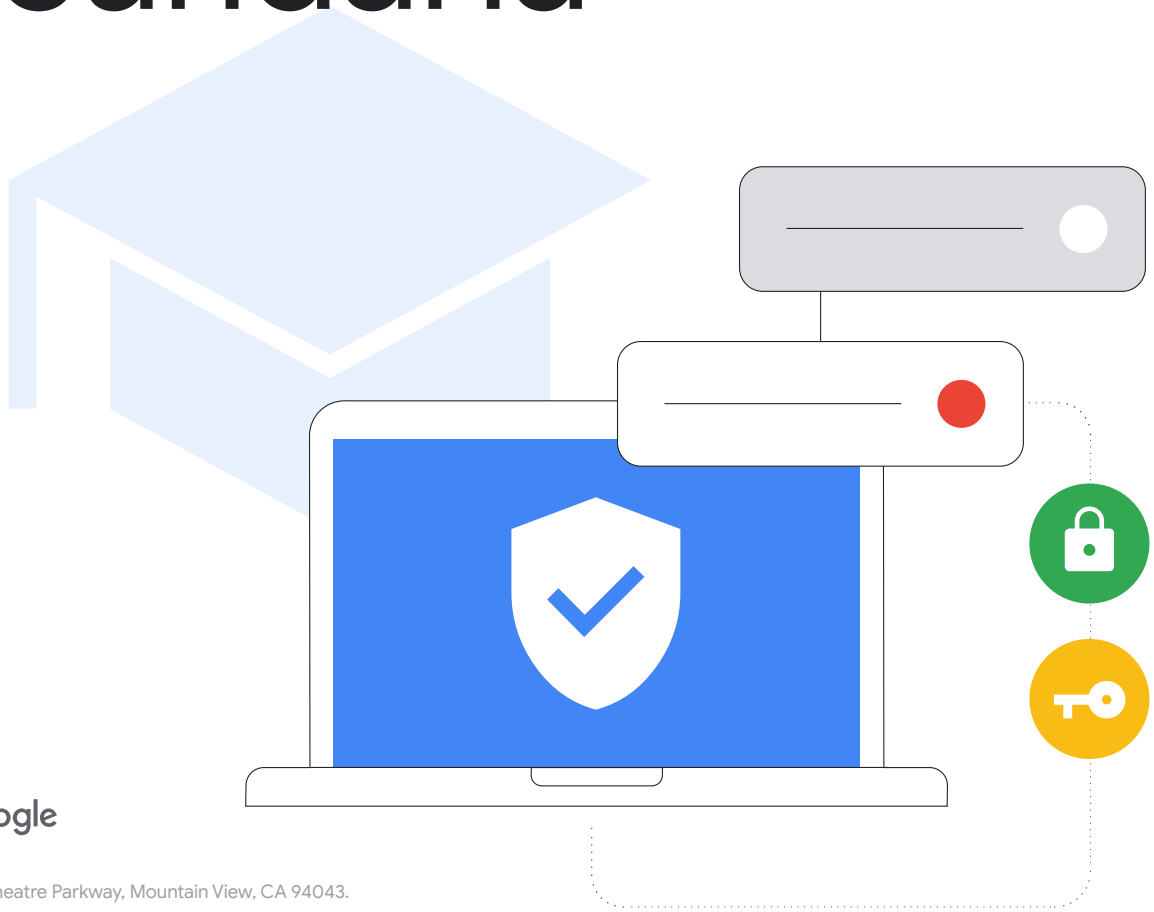
Google for Education

Actualización de la guía de ciberseguridad para enseñanza primaria y secundaria



Safer with Google

Resumen ejecutivo

Tal y como se destaca en el informe Protecting Our Future[1] de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA), es fundamental que las instituciones de enseñanza primaria y secundaria inviertan en ciberseguridad para proteger a los alumnos y sus familias, a los docentes, al personal y a las comunidades. En este documento para administradores de TI se ofrecen directrices y prácticas recomendadas sobre la instalación y configuración de hardware y software en los centros de enseñanza primaria y secundaria para reforzar la ciberseguridad. Se incluyen prácticas recomendadas generales y directrices específicas sobre productos y servicios de Google. La misión de Google, organizar la información del mundo y hacer que sea accesible y útil de forma universal, es el motor de la labor que llevamos a cabo en el equipo de Google for Education: crear herramientas diseñadas para enseñar y aprender. En esta guía, compartimos diversas lecciones sobre esta labor.

Proporcionamos prácticas recomendadas, organizadas por asunto, con información minuciosa sobre la instalación, la configuración y las estrategias de mitigación de riesgos. También explicamos el enfoque de ciberseguridad que aplica Google a los servicios y, en especial, a las herramientas del ámbito educativo. Aunque en este documento se incluyen directrices detalladas que se pueden aplicar a los productos o servicios de cualquier marca, creemos que los nuestros ofrecen una protección superior de forma predeterminada contra los ataques más comunes.

Riesgos

Las instituciones educativas son uno de los principales objetivos de los ciberataques, mediante los que los agentes perniciosos tratan de explotar los entornos de los centros para acceder a la gran cantidad de datos que contienen y sacar provecho de ello. El 46 % de los centros educativos que aún no han sufrido ningún ataque creen que en algún momento lo sufrirán, puesto que los ataques de ransomware son cada vez más sofisticados y difíciles de interceptar. Además, el 42 % de estos centros consideran que los ataques de ransomware están tan extendidos que son sencillamente inevitables. La acuciante necesidad de implantar la educación a distancia en el 2020 contribuyó notablemente a la aparición de carencias de ciberseguridad, lo que dejó a los centros vulnerables frente a los ataques.

Defensa

Dichos ataques se pueden mitigar. Aunque ningún tipo de tecnología evita completamente los riesgos, el sector de la enseñanza y los proveedores de tecnología educativa pueden colaborar para adoptar e instaurar prácticas recomendadas con las que diseñar una estrategia segura e integral que permita reducir los riesgos de forma considerable. Las instituciones educativas pueden mejorar la gestión de riesgos y la mitigación de ataques incorporando las precauciones y las políticas adecuadas para proteger a los usuarios, los dispositivos y la privacidad de los datos.

Recomendaciones clave

- **USA LA AUTENTICACIÓN SEGURA** para proteger la información sensible, los correos, los archivos y otros tipos de contenido, así como para evitar que los usuarios no autorizados accedan a los sistemas educativos. Aplica las prácticas recomendadas sobre autenticación de usuarios, como el uso de contraseñas seguras, la verificación en dos pasos (2SV), las llaves de acceso y los gestores de contraseñas siempre que sea posible, sobre todo en el caso de los administradores de TI y el personal que trabaja con información sensible.
- **APLICA AJUSTES DE SEGURIDAD ADECUADOS** para proteger a los usuarios, los datos y el entorno. Aunque los productos de Google tienen mecanismos de seguridad integrados, es de vital importancia que los administradores también usen y configuren las redes y los sistemas debidamente para evitar riesgos. Para proteger los centros educativos, aplica los principios de confianza cero y de mínimos accesos: los usuarios solo deben tener acceso al software, los datos, las aplicaciones y los sistemas que necesitan para desempeñar su trabajo de forma eficaz.
- **ACTUALIZA Y MEJORA TUS SISTEMAS** para proteger a los usuarios de las amenazas más recientes. Usa sistemas operativos (SOs) y navegadores modernos, y comprueba que todos los dispositivos de los usuarios tengan instaladas las versiones de software más recientes (o versiones aprobadas estables a largo plazo) y que se actualicen automáticamente. Adoptar soluciones mejores y más seguras, como los Chromebooks, puede incrementar el grado de protección. Nunca jamás se ha detectado ransomware en ningún dispositivo ChromeOS.
- **USA SISTEMAS DE ALERTAS Y MONITORIZACIÓN EN TIEMPO REAL** para mejorar tu posición de seguridad y mitigar los posibles problemas de forma rápida. Puedes usar estas funciones integradas en el software de comunicación y colaboración principal, como Google Workspace for Education, o implementar soluciones independientes de monitorización y almacenamiento de registros de seguridad. Lleva un seguimiento exhaustivo de las actividades que tienen que ver con la red, los dispositivos, las aplicaciones, los usuarios y los datos de tu centro educativo. Monitoriza los inicios de sesión en las cuentas, el uso compartido de archivos, el volumen de correos electrónicos (en especial, los intentos de phishing y difusión de malware), la actividad de dispositivos y los cambios de configuración. Debes tener tu solución de alertas y monitorización siempre actualizada para recibir notificaciones sobre amenazas, sucesos críticos y cambios en el sistema.
- **ENSEÑA A LOS DOCENTES, AL PERSONAL Y A LOS ALUMNOS** a usar los dispositivos y el software de forma segura, a identificar posibles amenazas e informar sobre ellas, y a compartir datos adecuadamente para protegerlos frente a algunos de los ataques más habituales. Los centros educativos o los distritos escolares pueden usar materiales de formación ya preparados y de libre disposición, además de crear otros con su marca, con lo que tienen a su alcance un completo conjunto de recursos.

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Recomendaciones específicas para los usuarios de productos de Google: Google ofrece productos, como Google Workspace for Education y los Chromebooks, que pueden mejorar la ciberseguridad de los centros educativos y facilitar la adopción de todas estas recomendaciones. Cuando se combinan, conforman una solución integral que ayuda a proteger la privacidad de los usuarios y ofrecen una seguridad excepcional a las instituciones educativas.

Estas estrategias, junto con las directrices que se indican en este documento, sientan una base excelente para la seguridad de las instituciones de enseñanza primaria y secundaria.

A abordagem do Google para educação

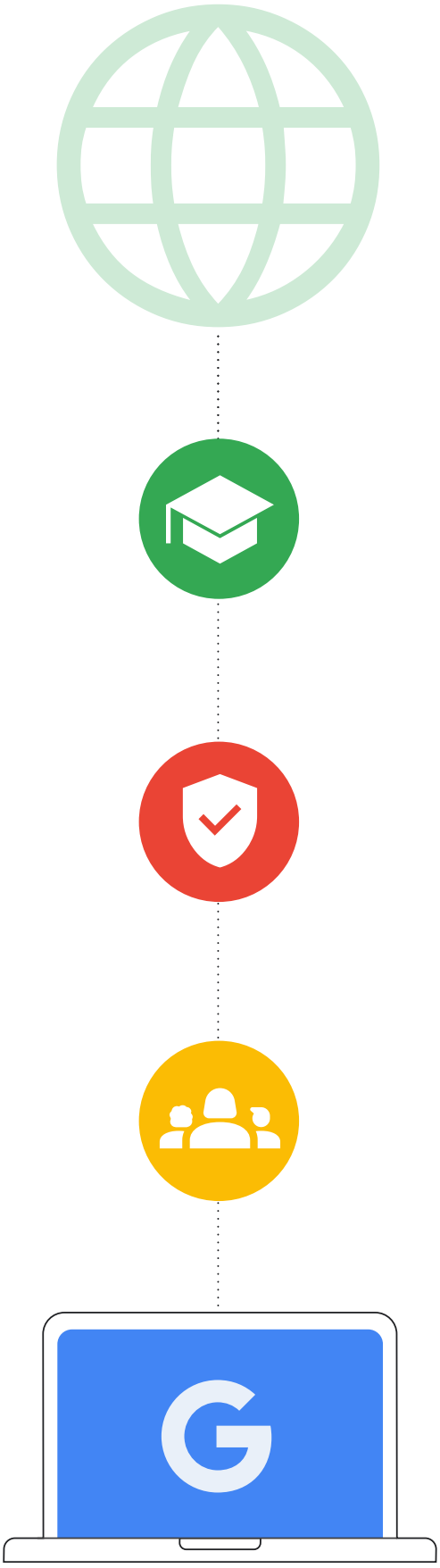
La misión de Google, organizar la información del mundo y hacer que sea accesible y útil de forma universal, abarca igualmente el sector educativo. Para cumplir esa misión, en el equipo de Google for Education desarrollamos soluciones, como los Chromebooks y Google Classroom, para que los alumnos y los docentes puedan crear, compartir y organizar su propio contenido, así como consultar y usar recursos didácticos y herramientas digitales de manera sencilla y segura.

Los centros educativos merecen disponer de tecnología con seguridad y privacidad integradas sobre la que puedan mantener el control y que les ofrezcan información y contenido de confianza. Gracias a productos como los Chromebooks y Google Workspace for Education, los centros disfrutan de soluciones de una seguridad extraordinaria que cumplen los estándares educativos internacionales más estrictos. Por su parte, los administradores de TI obtienen una visibilidad completa y un control sencillo de sus datos y políticas de seguridad. Por otro lado, los alumnos pueden sumergirse de lleno en la experiencia de aprendizaje mediante un entorno digital más seguro que proporciona contenido según la edad y mitiga el spam y las ciberamenazas.

Para garantizar un aprendizaje seguro para todos los usuarios, nuestra prioridad ha sido integrar controles y funciones de seguridad, cumplir los estándares de privacidad más estrictos y proporcionar opciones para que las herramientas de seguridad sean más proactivas. Los dispositivos ChromeOS ayudan a mitigar las amenazas a las que se enfrentan los centros educativos y son la mejor defensa contra la más común de ellas, el ransomware, hasta el punto de que ningún Chromebook ha sufrido nunca un ataque de este tipo.

Por su parte, Google Workspace for Education es uno de los paquetes de comunicación y colaboración basados en la nube más populares y seguros del mundo. Para obtener más información sobre cómo refuerza la ciberseguridad cada solución en relación con las recomendaciones recogidas en este documento, consulta la última sección.

Esta publicación consta de dos secciones. En la primera, se dan directrices prácticas y generales sobre la seguridad en las instituciones de enseñanza primaria y secundaria que se pueden aplicar a productos de cualquier marca. En la segunda, se ofrecen directrices de configuración específicas para las instituciones que usan productos de Google for Education, como Chromebooks y Google Workspace for Education. Ambas secciones proporcionan información para protegeros a ti y a tus alumnos en Internet.



Introducción

Tanto los dispositivos como las redes de las instituciones de enseñanza primaria y secundaria corren un riesgo alto de sufrir ciberataques, así que es crucial que incorporen los mejores mecanismos de seguridad posibles para proteger a los alumnos y evitar la pérdida de datos, servicios, recursos, tiempo y dinero que puede derivarse de dichos ataques (Fuente).

Esta guía es una herramienta para promover que los administradores y los sistemas de los centros educativos implementen prácticas de ciberseguridad que protejan mejor sus entornos. Al hacerlo, las instituciones de enseñanza primaria y secundaria pueden evitar que los sistemas educativos sufran ciberataques graves y costosos (o, al menos, mitigarlos), y proteger así a los alumnos, las familias, los docentes y el personal.

Los ciberataques contra centros educativos son cada vez más frecuentes y graves. Según K-12 Cybersecurity Resource Center, entre el 2016 y el 2021 se revelaron públicamente más de 1300 incidentes cibernéticos contra organizaciones educativas de los 50 estados de EE. UU. Los responsables del sector educativo deben proteger los datos y la información personal de los alumnos, los docentes y el personal, así como los sistemas y la información de los centros de enseñanza. Esta es una tarea de gran envergadura, sobre todo si tenemos en cuenta que a este sector le suele costar más que a otros estar al día en cuestiones de ciberseguridad.

Cuando logran su objetivo, los ciberataques de ransomware, phishing, malware y otros tipos pueden derivar en brechas de seguridad de información personal identificable (IPI) a gran escala, pagos desorbitados (el importe de rescate medio se ha quintuplicado desde el 2020 hasta alcanzar los 812.260 $) e interrupciones prolongadas en la docencia y otras operaciones escolares. No hace mucho, se desconectó todo el sistema de un centro educativo debido a un ataque de ransomware, lo que tuvo un efecto dominó en toda la comunidad, ya que los alumnos no pudieron asistir a clase durante varios días seguidos. Mientras las organizaciones de enseñanza primaria tengan recursos y financiación limitados, seguirán siendo el objetivo principal de estos ataques a menos que se invierta en mejorar la ciberseguridad.

La ciberseguridad siempre es mejor cuando hay comunicación, colaboración y alianzas. El presente documento se basa en los consejos de seguridad de Google, el framework de ciberseguridad del Instituto Nacional de Normas y Tecnología (NIST) y las herramientas y recomendaciones de ciberseguridad para la enseñanza primaria y secundaria de CISA del 2023. Todas estas fuentes de prácticas de seguridad gozan de un amplio reconocimiento. En este documento se detallan medidas generales que los administradores de TI deberían tomar o valorar, se facilitan algunas de las directrices y prácticas recomendadas de Google y se hace referencia a consejos y servicios de seguridad que ofrecen otras empresas. Los administradores deberían revisar todas las directrices de seguridad que proporcionen las empresas correspondientes e implementar las más recientes, ya que cada empresa es la que mejor puede describir los productos de los que es responsable y los cambios que hayan podido producirse.

Antes de aplicar las recomendaciones que se indican más abajo, debes tener en cuenta los factores siguientes:

Cuestiones importantes

1. **El tipo de protección adecuada para tu alumnado.**
Cada centro educativo tiene necesidades concretas, y puede ser preciso aplicar medidas adicionales de privacidad y seguridad para proteger a ciertos grupos. Muchas herramientas de tecnología educativa tienen funciones que permiten configurar el acceso por edad para, por ejemplo, limitar el contenido inapropiado o garantizar la privacidad de la ubicación y los datos de contacto de los alumnos.

2. **Los tipos de datos que almacenas.**
Si almacenas datos sensibles, puede que debas cifrarlos o guardarlos en una ubicación independiente.

3. **Los tipos de dispositivos que usas y tu modelo de implementación.**
Los dispositivos y sus aplicaciones deberían actualizarse de forma automática para maximizar la seguridad, cifrar los datos y aislar las cuentas para que los usuarios solo tengan acceso a su propia información.

4. **Tu centro educativo, el distrito escolar o las políticas de la zona.**
Puede que tu centro aplique políticas específicas sobre el uso de la tecnología. Tendrás que comprobar que todos los mecanismos de seguridad estén configurados de conformidad con dichas políticas.

Cada día, Gmail bloquea
100 millones
de intentos de phishing.

Cada semana, Google identifica
300,000
sitios web no seguros.

Cada día
74 millones
de usuarios reciben ayuda del Gestor de Contraseñas de Google.

Cada año
700 millones
de personas refuerzan su protección con la Revisión de Seguridad.

Usa la autenticación segura

Disponer de una autenticación segura debe ser la máxima prioridad de los centros educativos y otras instituciones. En el cuarto trimestre del 2022, las cuentas sin credenciales o con credenciales poco seguras representaron el 48 % de todos los factores de riesgo de las brechas de seguridad. Hay una serie de recomendaciones clave que ayudan a verificar la identidad de los usuarios y a restringir el acceso a la información según su rol.

Los administradores de TI deberían implementar el uso obligatorio de la verificación en dos pasos o 2SV (también conocida como "autenticación de dos factores" o "2FA") y cambiar a la autenticación sin contraseña (es decir, mediante llaves de acceso) siempre que sea posible, especialmente en el caso de los usuarios que accedan de forma remota a los sistemas del centro educativo. Este tipo de verificación añade una capa de seguridad a las cuentas online, con lo que los atacantes lo tienen mucho más difícil para acceder a ellas.

Los centros educativos usan muchos tipos de dispositivos y modelos de implementación, y hay distintos niveles de aptitud técnica en un entorno de enseñanza primaria y secundaria. La seguridad de las cuentas y los dispositivos varía en función de los roles y tipos de usuario a los que se aplican las prácticas recomendadas definidas: administradores de TI; docentes, personal y alumnos mayores que usan dispositivos asignados, y alumnos más jóvenes que usan dispositivos compartidos. Más abajo analizamos las recomendaciones específicas para cada grupo.

Se pueden usar varios tipos de métodos de autenticación recomendados con la mayoría de las configuraciones:

- **Contraseñas seguras:**
  Define requisitos técnicos mínimos de complejidad y longitud de las contraseñas y, después, pide a los usuarios que definan la suya propia al iniciar sesión por primera vez de conformidad con esos requisitos. Las frases de contraseña largas son más seguras por su longitud y sus caracteres complejos. Los usuarios no deben estar obligados a cambiarlas con frecuencia, ya que esto provoca que usen contraseñas más simples o variaciones mínimas (como cambiar un solo carácter).
- **Verificación en dos pasos (2SV):**
  E ste tipo de verificación protege las cuentas con un segundo paso, que suele requerir que el usuario use algo que tiene, como una llave de seguridad o una aplicación del teléfono móvil que genere un código de verificación de un solo uso. Aunque cualquier método de 2SV incrementa la seguridad de las cuentas, los administradores no deberían recurrir a la recepción de códigos de verificación mediante mensajes de texto o llamadas, puesto que los números de teléfono pueden ser objetivos de ataques.
- **Autenticación sin contraseña:**
  Las llaves de acceso son una alternativa a las contraseñas más segura y sencilla. Los usuarios pueden iniciar sesión en aplicaciones y sitios web con PINs, patrones, sensores biométricos (de huella digital o reconocimiento facial, por ejemplo) o llaves de seguridad, con lo que no tienen que recordar ni gestionar contraseñas. Aunque estos métodos pueden no ser adecuados en todos los contextos educativos, cada vez se usan más en lugar de las formas de autenticación tradicionales y permiten iniciar sesión de forma más rápida y segura. Las llaves de acceso protegen a los usuarios de los ataques de phishing, ya que solo funcionan en los sitios web y las aplicaciones que se hayan registrado.
- **Inicio de sesión único (SSO):**
  Este método permite a los usuarios acceder a varias aplicaciones y sitios web con un solo conjunto de credenciales. Si los usuarios solo tienen que recordar un conjunto de credenciales, es menos probable que las apunten. Además, si los centros educativos no tienen que gestionar varios conjuntos de credenciales de usuario, pueden ahorrar en costes de asistencia de TI y del centro de asistencia. Google Workspace for Education admite el SSO de forma nativa, así que los usuarios pueden utilizar las credenciales de su cuenta de Google para iniciar sesión en aplicaciones de terceros, o utilizar las credenciales de otro proveedor para iniciar sesión en sus cuentas de Google.
- **Gestores de contraseñas:**
  Estas soluciones pueden ayudar a los usuarios a crear contraseñas únicas y seguras para las cuentas y servicios que usan cuando van a clase o hacen los deberes (si no usan el SSO). Estos gestores no ayudan a iniciar sesión en el sistema operativo de un dispositivo, sino que gestionan las contraseñas una vez que el usuario ha iniciado sesión. Los usuarios de Google pueden utilizar el Gestor de Contraseñas en Chrome con cualquier plataforma, ChromeOS y Android.

Los diversos grupos con necesidades específicas se beneficiarán de los subconjuntos especializados o las combinaciones de estas estrategias de autenticación, según su edad, su rol en el centro educativo y el tipo de sistemas y datos a los que tengan acceso.

Administradores de los centros educativos

Los administradores controlan los sistemas y una gran parte de los datos de las instituciones de enseñanza primaria y secundaria. Proteger sus cuentas es esencial para proteger todo el sistema, desde la infraestructura hasta los datos y los dispositivos que administra el centro. Por tanto, deben adoptar un estándar de referencia en materia de autenticación y, por ejemplo, usar contraseñas seguras, gestores de contraseñas eficaces y 2SV. Cada uno de estos mecanismos añade una capa de protección y, en combinación, proporcionan una seguridad máxima a la cuenta de administrador y los servicios empresariales.

- Los administradores deberían usar una llave de seguridad física o un método de 2SV con cifrado seguro que requiera un dispositivo de confianza y peticiones. Para ello, se puede recurrir a un servicio como Google Authenticator u otra aplicación que genere códigos de verificación de un solo uso. Los Chromebooks que se lanzaron después del 2019 con un chip TPM incluyen un botón de encendido, que se puede utilizar para llevar a cabo la autenticación de dos factores.
- Los administradores deberían usar un gestor de contraseñas de confianza compatible con 2SV para almacenar las contraseñas de distintos servicios.

Docentes y personal que usan dispositivos asignados

Al igual que los administradores, los docentes y el personal tienen acceso a datos sensibles, pero no tienen el control de la infraestructura digital y sus aptitudes técnicas son más diversas.

- Los docentes y el personal con Chromebooks deberían tener la opción de iniciar sesión mediante verificación biométrica (por ejemplo, mediante huella digital) en los casos en que lo permita la ley.
- Los administradores deberían implementar el uso obligatorio de 2SV y cambiar a la autenticación sin contraseña siempre que sea posible, especialmente en el caso de los miembros del personal que accedan de forma remota a los sistemas del centro educativo.

Alumnos mayores que usan dispositivos asignados (normalmente, a partir de 4.º curso)

Los alumnos de mayor edad han recibido más formación sobre cómo protegerse y suelen ser capaces de usar mecanismos de autenticación más seguros y adecuados para los tipos de servicios que probablemente tengan que usar. Solo deberían tener acceso a su propia cuenta y a la información que se haya compartido con ellos.

- Los alumnos con Chromebooks deberían tener la opción de crear un PIN específico para el dispositivo con el que iniciar sesión más rápidol. Puede que las opciones biométricas no sean adecuadas o factibles en muchos entornos escolares.
- Todos los alumnos deberían recibir asistencia para crear una contraseña única que no incluya información personal (como su nombre, el número de su aula o su cumpleaños). Se debería enseñar a los alumnos que las frases de contraseña aportan complejidad y, a su vez, son fáciles de recordar.

Alumnos más jóvenes que usan dispositivos compartidos (normalmente, desde infantil hasta 3.º)

A los alumnos de menor edad, que aún están aprendiendo a usar la tecnología educativa, les convendrá usar una autenticación sencilla, que además es adecuada cuando los servicios y los datos a los que se accede son limitados

- Los centros educativos que usan métodos de terceros sin contraseña (como códigos QR o inicio de sesión mediante imágenes) para los alumnos más pequeños o los que no pueden usar contraseñas deberían adoptar precauciones específicas, puesto que estos son menos seguros. Los administradores deberían cambiar la contraseña de un alumno y actualizar el código si este se ha perdido o se ha expuesto a otras personas.
- Los centros educativos deben enseñar a los alumnos y a sus padres lo importante que es mantener las contraseñas en secreto y guardar las credenciales alternativas (como los códigos QR) de forma segura.
- En el caso de los dispositivos asignados, como las tablets, se puede usar un PIN específico para el dispositivo a modo de método de autenticación alternativo.

Aplica ajustes de seguridad adecuados

Los dispositivos y las redes del sector educativo son objetivos con mucho valor y visibilidad para los atacantes de todo el mundo. Por ello, es vital que dispongan de la máxima seguridad posible para evitar la interrupción de servicios y la pérdida de recursos, tiempo y dinero. Aparte de incorporar funciones de seguridad eficaces y compatibles con los productos que se usan en el centro, los administradores de los sistemas deben procurar que a los docentes, el personal y los alumnos les resulte fácil manejarlos. Los ajustes de seguridad y privacidad importantes deben configurarse de tal forma que los usuarios no puedan inhabilitarlos ni modificarlos. Además, en el caso de otros ajustes, los administradores deben asignarles valores por defecto que protejan a los usuarios. Es vital disponer de la máxima seguridad posible para evitar la interrupción de los servicios y la pérdida de recursos, tiempo y dinero. Si usas Chromebooks, en la última sección puedes consultar nuestras sugerencias de configuración de políticas de dispositivos.

Por último, integra la minimización de datos en tus prácticas recogiendo, usando o revelando información personal únicamente para los propósitos y por los medios que sean razonablemente necesarios y proporcionales para prestar el servicio, o bien de un modo que sea acorde al contexto de la relación.

Aplicaciones y actualizaciones

Limita y minimiza las aplicaciones que pueden instalar tus usuarios en los dispositivos, puesto que cada una de ellas es un posible vector de ataque que se puede aprovechar. Si es posible, usa aplicaciones de fuentes de confianza. Por ejemplo, recomienda a los usuarios que busquen la insignia de verificación en Google Play Store para tener la certeza de que descargan aplicaciones oficiales que hayan superado las revisiones de seguridad. Las modificaciones de SO o de hardware (jailbreaking o rooting) provocan problemas de seguridad graves, así que deben evitarse.

Acceso y visibilidad

Los administradores deben comprobar que los usuarios solo tengan acceso a los datos, al software, a los servicios y a los sistemas que necesitan para hacer su trabajo o aprender de forma eficaz. Esta medida permite restringir los accesos accidentales y saber qué usuarios tienen acceso a qué recursos. Presta especial atención a los datos muy sensibles (como la IPI de los usuarios) y a los sistemas (como los de RR. HH., gestión de nóminas, calificación, seguridad y configuración) examinando qué usuarios pueden acceder a ellos y en qué circunstancias. Limita también el acceso a los dispositivos que sean propiedad del centro y comprueba que solo ciertos miembros del personal tengan acceso a ellos.

Revisa las políticas de uso compartido de datos en herramientas de colaboración para evitar que se divulguen demasiados datos, que se transmitan a usuarios inadecuados o que se consulten sin autorización. Limita o impide la posibilidad de compartirlos fuera del entorno (especialmente por parte de los alumnos) e instaura políticas para monitorizar la difusión de contenido sensible.

Pérdida o robo de dispositivos

Perder un dispositivo no implica necesariamente la pérdida de datos. Los administradores deberían establecer un protocolo para que se pueda acceder a la información y los documentos de un dispositivo en caso de que se pierda o lo roben. Por ejemplo, los documentos se pueden almacenar en un entorno en la nube. Descarga e imprime los códigos de verificación alternativos de tus procesos de 2SV para evitar que se interrumpa el acceso a las cuentas.

Cuando se notifica la pérdida o el robo de un dispositivo, comprueba que se haya bloqueado de forma remota (si es posible) y que las cuentas asociadas se hayan bloqueado o identificado para impedir que se produzcan accesos no autorizados a través de ellas. El contenido de los Chromebooks puede borrarse de forma remota si estos se pierden, y las cuentas de Google Workspace for Education pueden monitorizarse para detectar actividad sospechosa o suspenderse (bloquearse) en caso necesario.

Protección avanzada para usuarios de alto riesgo

Para los usuarios muy visibles y con información sensible (como los administradores de Google Workspace for Education), Google dispone del Programa de Protección Avanzada (APP). Este programa ofrece una mayor protección frente a los ataques dirigidos, como los intentos de phishing, las descargas maliciosas y las vulneraciones de contraseñas. Está diseñado específicamente para frustrar ataques online dirigidos a cuentas de Google, aplica de forma automática la autenticación segura y llaves de seguridad, y restringe el acceso de terceros a los datos de las cuentas. Otros proveedores de cuentas online también ofrecen mecanismos seguros de protección para usuarios de alto riesgo, mecanismos que los administradores y el personal que tenga acceso a información personal o sistemas tecnológicos siempre deberían usar.

Actualiza y mejora tus sistemas

Una de las medidas más importantes que puedes tomar para protegerte es tener las aplicaciones y el sistema operativo de los dispositivos siempre actualizados. Esto cobra mayor relevancia, si cabe, en los centros de enseñanza primaria y secundaria, puesto que son una parte fundamental de la educación y la vida cotidiana de los niños. La mayoría de los ataques de malware que se producen en entornos educativos y otros contextos de alto riesgo se basan en Windows, como el que sufrió SolarWinds, el ataque de ransomware contra el distrito escolar unificado de Los Ángeles, el hackeo del distrito escolar de Little Rock, la brecha de seguridad de datos de Microsoft Exchange Server, el ataque de ransomware contra el distrito escolar de Albuquerque y la reciente brecha de seguridad de cuentas de agencias federales de Microsoft. Este es otro ámbito en el que los productos y servicios basados en la nube pueden facilitar las tareas de los administradores, puesto que la superficie de ataque se reduce y los sistemas y aplicaciones se actualizan de forma automática.

Cambia a un sistema operativo moderno y mantenlo actualizado

La versión más reciente de un SO suele contener funciones de seguridad nuevas que ayudan a evitar vectores de ataques conocidos. Deberías habilitar la actualización automática del SO del dispositivo. Si esto no es posible, debes descargar e instalar parches y actualizaciones de un proveedor de confianza al menos una vez al mes.

Los Chromebooks ejecutan ChromeOS, así que reciben con frecuencia actualizaciones automáticas con los parches de seguridad más recientes para adoptar innovaciones de seguridad con rapidez. Además, verifican la integridad del SO (de solo lectura) antes de iniciarse. También cifran todos los datos almacenados en el dispositivo, lo que los protege de accesos no autorizados, y ejecutan todas las páginas web y aplicaciones en un entorno aislado. Así, si un sitio web o una aplicación están infectados con malware, este no puede propagarse a otras áreas del dispositivo.

Si tu centro no está listo para adoptar Chromebooks, ChromeOS Flex es una versión de ChromeOS diseñada para modernizar dispositivos escolares. ChromeOS Flex proporciona a todo el mundo una experiencia de enseñanza y aprendizaje moderna y unificada, con seguridad proactiva e integrada y capacidades de gestión basadas en la nube. ChromeOS Flex puede ofrecer una protección automatizada y bloquear aplicaciones y ejecutables maliciosos sin reemplazar el hardware que tienes.

Cambia a un navegador moderno y mantenlo actualizado

Es muy importante que el navegador también esté actualizado y sea seguro. Los navegadores modernos ofrecen funciones de seguridad más avanzadas que las cuales ayudan a proteger la información sensible que se transfiere por Internet. Pueden habilitarlas los usuarios tras pedírselo el propio navegador o configurarlas los administradores de modo que se activen de forma predeterminada en los ordenadores de los centros docentes. El navegador debe mantenerse actualizado. Ya se use para trabajar, aprender o hacer cualquier otra actividad online, un navegador moderno actualizado se caracteriza por lo siguiente:

- **Usar métodos de seguridad eficaces**, como el aislamiento de sitios web y la protección de navegación segura para evitar que los usuarios accedan sin querer a sitios web peligrosos.
- **Tener habilitadas las actualizaciones automáticas** para que el navegador reciba actualizaciones de seguridad con rapidez.
- **Comprobar que la conexión sea segura** mediante la seguridad en la capa de transporte que debe usar. Los usuarios pueden hacer clic junto a la URL para consultar si la conexión se ha marcado como segura.

Chrome se ha diseñado pensando en la seguridad y tiene funciones activadas de forma predeterminada, como Navegación Segura. También integra un gestor de contraseñas que permite autocompletar contraseñas mientras se navega por la Web, lo que facilita el uso de contraseñas seguras.

Usa sistemas de alertas y monitorización en tiempo real

Los sistemas de alertas y monitorización en tiempo real pueden ayudar a los centros educativos a identificar amenazas y atajarlas con rapidez antes de que causen daños. Es esencial comprobar que las herramientas de seguridad se estén ejecutando en segundo plano para registrar las actividades relacionadas con la seguridad de todos tus sistemas. Las herramientas de inteligencia artificial (IA) son muy eficaces analizando grandes volúmenes de datos recogidos e identificando anomalías y patrones. Esta información se puede usar para detectar amenazas de forma más rápida y sencilla, así como para procesar y solucionar las vulnerabilidades. Además, esta tecnología permite priorizar las actividades que deben revisar el personal o el administrador de TI.

Los centros educativos pueden usar las funciones de alertas y monitorización integradas en su software de comunicación y colaboración principal, como Google Workspace for Education, o implementar soluciones independientes de gestión de información y eventos de seguridad (SIEM).

Los sistemas de alertas y monitorización en tiempo real pueden llevar un seguimiento de diversas actividades que tienen que ver con la red, los dispositivos, las aplicaciones, los usuarios y los datos de tu centro educativo, como los inicios de sesión de los usuarios, el acceso a archivos, posibles intrusiones, robos de datos o intentos de robo, y actividades de los administradores.

Si el sistema detecta actividades sospechosas, puede enviar una alerta al personal de TI del centro educativo. Así, los administradores pueden investigar el problema y tomar medidas para mitigar la amenaza.

Además, las herramientas de alertas y monitorización sirven para obtener más información sobre las amenazas a las que se enfrentan los centros educativos. Al analizar los datos de estos sistemas en tiempo real, los centros pueden identificar tendencias y patrones para protegerse mejor.

A continuación, se muestran algunas prácticas recomendadas para usar los sistemas de alertas y monitorización (incluidos los de SIEM):

1. **Fija tus objetivos de seguridad**
   Identifica qué información y sistemas son más esenciales para el centro educativo y qué tipos de amenazas los podrían poner en mayor riesgo. Después, trata de identificar los datos que debes recoger para monitorizar la aparición de esas amenazas.

2. **Recoge los datos correctos y usa configuraciones adecuadas**
   EEs importante que recojas los datos correctos y que configures las aplicaciones de forma adecuada para abordar los objetivos de seguridad más pertinentes. Los datos pueden proceder de cortafuegos, filtros de contenido, sistemas de detección de intrusos, servidores web y otros dispositivos de seguridad, así como software de comunicación y colaboración, sistemas de información sobre alumnos y plataformas de aprendizaje online.

3. **Investiga las alertas y toma medidas**
   Cuando tu sistema de monitorización genere una alerta, es importante que investigues el problema y actúes en consecuencia. Puede que tengas que recurrir a varios equipos para investigar el origen de la alerta y, o bien determinar si es un falso positivo, o bien tomar medidas para mitigar la amenaza, como suspender cuentas, cambiar contraseñas de usuarios, poner en cuarentena o eliminar correos, cambiar permisos de archivos o borrar dispositivos.

Enseña a los docentes, al personal y a los alumnos

Las instituciones de enseñanza primaria y secundaria deberían fomentar la concienciación y hábitos de seguridad en las comunidades escolares mediante campañas y colaboraciones para empoderar a sus usuarios. Enseñar a los docentes, al personal y a los alumnos lo importante que es la seguridad es esencial para ayudarles a protegerse en Internet. Además, contribuye a prevenir ciberamenazas graves. Enséñales a usar los productos y servicios que ofrece la institución, a detectar y notificar amenazas como los correos de phishing y, lo que es más importante, a tomar medidas para evitar ataques. Los centros educativos y los distritos deberían fomentar la concienciación y hábitos de seguridad en las comunidades escolares mediante campañas y colaboraciones para empoderar a sus usuarios.

Usar dispositivos y software de forma segura

Los administradores pueden colaborar con los docentes y expertos para elaborar planes de estudios sobre ciberseguridad acordes a la edad de los alumnos para que aprendan a usar dispositivos, software y sistemas de forma segura. Crear materiales de formación con la marca del centro educativo o el distrito escolar ayuda a contextualizar las recomendaciones para los docentes y los alumnos. No obstante, también puedes aprovechar materiales ya preparados, como el sitio web Sé genial en Internet (disponible en Safety.Google), y los materiales de Khan Academy, y adaptarlos a tus necesidades. Estos programas pueden ayudar a tus usuarios a protegerse estén donde estén, ya sea en el centro educativo o en otro contexto de la comunidad.

Reconocer amenazas

Formar a los docentes, al personal y a los alumnos para que sepan reconocer las amenazas es fundamental para su seguridad. Es importante enseñar a los niños a detectar si algo es una amenaza o no, puesto que puede que no sepan identificar si lo que tienen delante es legítimo. Hay una serie de amenazas que deben saber reconocer y notificar, y los administradores deberían centrarse en las cuestiones que crean que pueden ofrecer un mayor retorno de la inversión. Cabe señalar que no solo se ha de enseñar a reconocer amenazas, sino también a tomar medidas. Las amenazas más comunes que deben reconocer los usuarios son el ransomware, el phishing, la ingeniería social, el malware y las estafas. Sin embargo, si en un centro predominan otras amenazas, la comunidad escolar debe recibir formación al respecto.

Compartir datos y archivos de forma segura

Los docentes y el personal deben recibir formación sobre cómo compartir datos y archivos de forma adecuada y cómo reconocer las solicitudes indebidas que llegan por correo electrónico. Por encima de todo, la información personal sensible solo se transmitirá o tratará en los casos necesarios y siempre que tenga varias capas de protección. Por ejemplo, nunca habrá de compartirse por correo ni con destinatarios externos. Los docentes y el personal deben usar funciones de prevención de la pérdida de datos (incluidas en ChromeOS y Workspace for Education) para advertir a los usuarios finales y evitar que compartan archivos con datos sensibles (como números de identificación personal) o copien contenido sensible y lo peguen fuera del dominio.

La estrategia de Google en acción: dispositivos y servicios para el sector educativo

El aprovisionamiento de software es una de las medidas más eficaces que puede tomar un distrito escolar para protegerse. El software debe tener una arquitectura sólida y un diseño que minimice el riesgo de sufrir vulnerabilidades, así como integrar la seguridad en cada capa. Si se exige a los centros educativos que compren software seguro o de empresas con una trayectoria de compromiso con la seguridad, el riesgo cibernético general puede reducirse de forma notable. En Google, hemos reforzado ChromeOS y seguimos implementando soluciones más proactivas e inteligentes que aprovechan el potencial del aprendizaje automático, la nube y los conocimientos sobre identidad que poseemos.

Nuestro compromiso es crear productos que ayuden a proteger la privacidad de los alumnos y los docentes y que ofrezcan una seguridad excepcional a los centros educativos. Puedes depositar tu confianza en los productos y servicios de Google for Education, puesto que protegen continuamente a los usuarios, dispositivos y datos frente a amenazas cada vez más complejas. En esta sección, se ofrece una guía para los administradores de TI con recomendaciones de seguridad para usar los productos de Google for Education.

Google Workspace for Education

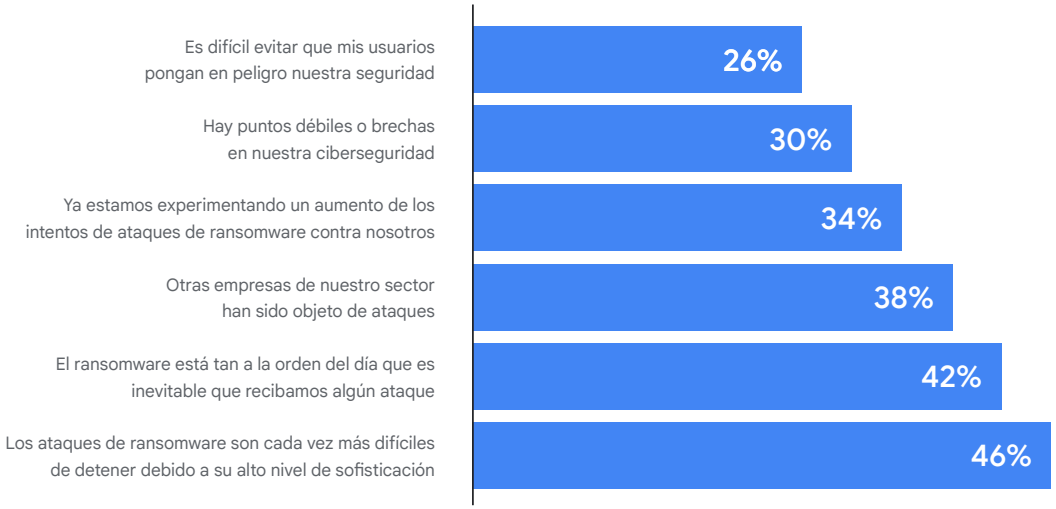
Google Workspace for Education es un conjunto de herramientas y servicios de Google ideado para que los centros educativos puedan colaborar, dinamizar la enseñanza y garantizar un aprendizaje seguro. Los productos y servicios de Google for Education protegen continuamente a los usuarios, dispositivos y datos frente a amenazas cada vez más complejas. Además, proporcionan centros de alertas y seguridad, un almacén para descubrimientos electrónicos, herramientas de gestión de identidades y accesos, y funciones para prevenir la pérdida de datos.

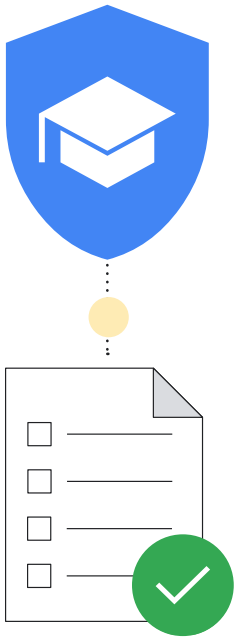
Hemos elaborado materiales que te servirán de ayuda si estás empezando a usar Google Workspace for Education. Muchos de ellos pueden ayudarte a configurar los ajustes de conformidad con las recomendaciones que te damos en esta guía. Si necesitas ayuda para empezar a usar Google Workspace for Education, consulta la Guía de inicio rápido para configurar el sistema de TI.

Consulta las listas de comprobación de seguridad

Consulta las listas de comprobación de seguridad para obtener más información sobre cómo reforzar la protección y la privacidad de tu institución. Si tu centro educativo tiene la edición Standard o Plus de Google Workspace for Education, puedes usar la página Estado de seguridad para monitorizar la configuración de la consola de administración. Asimismo, puedes verificar el estado de diversos ajustes, como el reenvío automático de correos, el cifrado de dispositivos, las opciones para compartir de Google Drive y mucho más. Si te hace falta, también puedes ajustar la configuración de tu dominio en función de las directrices generales y las prácticas recomendadas de seguridad para adaptarla a las necesidades comerciales y a la política de gestión de riesgos de tu organización, aunque siempre debes seguir estas directrices.

Por qué el sector educativo espera recibir ataques





Fuente: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

A continuación, se muestran más consejos de seguridad para que aproveches al máximo las protecciones integradas en Google Workspace for Education:

Añade unidades organizativas (UOs)

No cabe duda de que todos los usuarios de tu cuenta de Google Workspace for Education deben tener la misma configuración. Las UOs son grupos de usuarios a los que puedes asignar servicios, ajustes y permisos específicos. Por ejemplo, puedes usar la 2SV con el profesorado y el personal, y distintos métodos de autenticación acordes a la edad con los alumnos más jóvenes. Añade UOs independientes para los docentes, el personal y los alumnos; así podrás aplicar políticas distintas a cada grupo de usuarios. Contar con una estructura bien diseñada es esencial para poder gestionar tu cuenta de Google Workspace for Education de forma eficaz y flexible.

Implementa políticas de contraseñas y protecciones para cuentas de administrador

Como hemos visto, la autenticación de los usuarios es esencial para mantener la institución a salvo. Por ello, ofrecemos formas flexibles de gestionar la autenticación de los administradores que te permiten proteger debidamente las cuentas de los usuarios. Aplica políticas de contraseñas para que los usuarios creen contraseñas seguras y valora el uso obligatorio de la 2SV cuando sea conveniente según las recomendaciones sobre grupos que figuran en la sección sobre inicio de sesión seguro. Puedes implementar el uso obligatorio de 2SV por parte de un grupo de usuarios (dales tiempo para que la configuren) e implementar esta verificación mediante diversos métodos, como las llaves de seguridad (protección máxima), una notificación de Google (de aplicaciones de Google para Android y iOS), aplicaciones de generación de códigos de verificación (como Google Authenticator) y mensajes de texto o llamadas de teléfono (aunque son el método menos seguro).

Aunque utilices proveedores de identidades (IdP) distintos a Google en tu organización, puedes configurar el inicio de sesión único (SSO). Además, puedes aplicar la 2SV con SSO a cuentas que no sean de superadministrador si lo prefieres.

Activa o desactiva servicios

Desde la consola de administración de Google, los administradores pueden controlar a qué servicios de Google pueden acceder los usuarios con sus cuentas de Google Workspace for Education. Puedes controlar el acceso a servicios de Google, como Calendar, Drive y Meet, activándolos o desactivándolos para cada UO (también puedes activar servicios si usas grupos). Además, puedes consultar las diferencias entre los servicios principales de Workspace y los servicios adicionales antes de activar servicios adicionales como YouTube, Google Maps y Blogger. Es recomendable que los administradores controlen el acceso a los servicios de Google por edad y tengan en cuenta que a los usuarios designados como menores de 18 años se les aplicarán restricciones de forma automática en algunos servicios de Google cuando hayan iniciado sesión en sus cuentas de Google Workspace for Education.

También puedes usar el acceso contextual (disponible en Workspace for Education Standard y Plus) para permitir o bloquear el acceso a las aplicaciones de Google, como Gmail, Drive y Calendar, en función de la dirección IP, el origen geográfico, las políticas de seguridad o el SO de un dispositivo. Por ejemplo, puedes permitir que se utilice Drive para ordenadores solo en dispositivos que sean propiedad de la empresa y estén en determinados países o zonas.

Métodos para dar a los usuarios acceso a servicios

En la consola de administración de Google, puedes desactivar el acceso de una unidad organizativa a un servicio de Google, como Google Drive. Si algunos usuarios de esa unidad organizativa necesitan utilizar Drive, tienes dos opciones:

1. Mover a los usuarios a una unidad organizativa que tenga Drive activado.
2. Añadir a los usuarios a un grupo de acceso y activar Drive para el grupo. Cada miembro puede acceder al servicio, incluso si su unidad organizativa lo tiene desactivado.

Google Drive está desactivado en las unidades organizativas 1 y 2.

No obstante, un **grupo de usuarios** de las unidades organizativas 1 y 2 puede utilizar Google Drive.

Fuente: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Implementa políticas de uso compartido y reglas de conservación de datos

Como administrador, puedes controlar si los usuarios pueden compartir archivos y carpetas de Google Drive con usuarios que no pertenezcan a la organización. Este control contribuye a evitar que se compartan demasiados datos y archivos, o que se haga de forma accidental, lo que previene las filtraciones de datos. Separar los archivos de las unidades, crear unidades organizativas y aplicar el principio de mínimos accesos son medidas importantes para evitar que los atacantes se desplacen de una red a otra si se infiltran en una cuenta. Cuanto más limitado sea el acceso a datos y redes de un posible atacante, menos daño podrá causar.

Desactiva las opciones correspondientes para impedir que los alumnos puedan compartir archivos con usuarios externos (o permite que solo se puedan compartir con determinados dominios) y asigna el valor Solo destinatarios a "Access Checker". Si permites que algunos o todos los usuarios compartan archivos con usuarios ajenos a tu dominio, activa una advertencia para cuando un usuario vaya a hacerlo. Además, desactiva la publicación de archivos en la Web y pide a tus colaboradores externos que inicien sesión con una cuenta de Google.

Por otra parte, los clientes de Workspace for Education Standard y Plus pueden usar audiencias objetivo y reglas de confianza para aplicar recomendaciones y restricciones de uso compartido de forma más precisa. Por ejemplo, con las audiencias objetivo puedes definir que la audiencia por defecto con la que el profesorado pueda compartir enlaces esté compuesta por los docentes y el personal, en lugar de todos los usuarios de la institución. Con las reglas de confianza, puedes impedir que los alumnos de primaria compartan archivos con alumnos más mayores.

Revisa las políticas de unidades compartidas para comprobar que solo los usuarios adecuados puedan crear unidades compartidas y evitar que los usuarios externos accedan a ellas. Es recomendable que solo permitas crear unidades compartidas a los administradores (o al personal y los docentes) y que gestiones el acceso a las unidades compartidas cuidadosamente.

Valora limitar la visibilidad del directorio y el uso compartido de contactos siempre que sea posible. Para ello, puedes desactivar el uso compartido de contactos para algunos o todos los usuarios, o bien crear directorios personalizados para controlar qué usuarios pueden ver qué contactos.

Implementa políticas de prevención de la pérdida de datos (DLP) en Drive y Gmail para detectar información sensible y bloquearla. Existen políticas prediseñadas que puedes usar para proteger información sensible de uso común (como números de cuentas bancarias o de tarjetas de crédito). También puedes crear políticas personalizadas según palabras clave, listas de palabras y expresiones regulares (regex).

Gestiona la configuración de Gmail

Gmail, que es uno de los servicios principales de Google Workspace for Education, dispone de muchos ajustes que los administradores pueden aprovechar para proteger su institución y a sus usuarios.

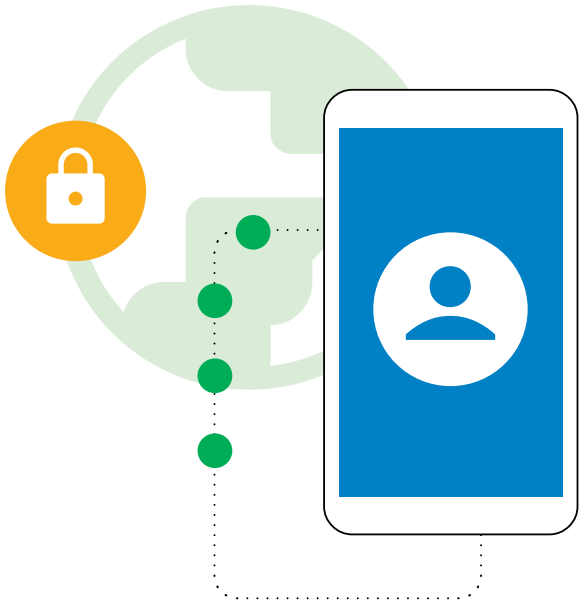
Evita el spam, el spoofing y el phishing con la autenticación de Gmail. Puedes personalizar los filtros de spam para que, por ejemplo, sea obligatoria la autenticación del remitente en el caso de los remitentes aprobados o para desactivar la opción de evitar los filtros de spam en el caso de los remitentes internos.

Desactiva el acceso POP e IMAP si es posible y activa el análisis mejorado de mensajes antes de la entrega y la protección avanzada contra phishing y malware. Si permites que algunos o todos los usuarios reciban correos externos, puedes habilitar advertencias sobre destinatarios externos.

Los clientes de Google Workspace for Education Standard y Plus también pueden protegerse mejor del malware y el ransomware configurando reglas para detectar archivos adjuntos dañinos mediante Entorno Aislado de Seguridad.

Aprueba aplicaciones de terceros

Usa flujos de trabajo integrados para aprobar aplicaciones de terceros que accedan a los datos de cuentas mediante APIs. Esta medida ayuda a evitar que se compartan datos no autorizados con aplicaciones de terceros cuyo uso escolar no se haya aprobado.



Usa informes y la monitorización

Como administrador, puedes consultar informes y eventos de registro en la consola de administración de Google para revisar la actividad de tu organización, como posibles riesgos de seguridad, qué usuarios inician sesión y cuándo, y cómo crean y comparten contenido. Por medio de tablas y gráficos, puedes consultar datos relativos al dominio, así como información más detallada sobre los usuarios. Consulta informes y registros de auditoría (y el Centro de alertas) para identificar riesgos de seguridad, analizar el uso de los servicios, diagnosticar problemas de configuración, llevar un seguimiento de la actividad de los usuarios y mucho más.

Los administradores de Google Workspace for Education Standard y Plus pueden consultar el panel de seguridad para obtener una vista general de distintos informes de seguridad, identificar tendencias y comparar los datos actuales con los del historial; por ejemplo, sobre el uso compartido de archivos en Drive, la actividad de spam, phishing y malware en Gmail, los inicios de sesión sospechosos en cuentas de usuarios y la actividad de dispositivos sospechosa. La mayoría de los datos de uso, la actividad y los registros de auditoría (lo que incluye los eventos de registro de administrador, Drive, Meet y Chat), así como los informes de seguridad, están a tu disposición durante seis meses.

Aprovecha el Centro de Seguridad

LLos administradores de Google Workspace for Education Plus y Standard pueden usar el Centro de Seguridad, que ofrece estadísticas e información de seguridad avanzada, así como visibilidad añadida y control sobre los problemas de seguridad que afectan al dominio.

El Centro de Seguridad incluye la herramienta de investigación de seguridad, que puede ayudar a los administradores a identificar, clasificar y tomar medidas para abordar problemas de seguridad y privacidad, como ataques de phishing, intercambios inadecuados de archivos y actividades sospechosas de usuarios y dispositivos, entre muchos otros.

Google Workspace es el paquete de comunicación y de colaboración nativo de la nube más seguro del mundo

0

vulnerabilidades de software explotadas activamente en Workspace desde noviembre del 2021*

50%

de ahorro potencial en primas de seguros de ciberseguridad al usar Workspace

2x menos

de incidentes de seguridad en las empresas que usan Workspace en comparación con Microsoft 365

2.5x menos

de incidentes de seguridad en las empresas que usan Workspace en comparación con Microsoft Exchange

* Según CISA, se trata de una cifra muy inferior a la de cualquier otro proveedor de soluciones de productividad en este espacio.

Chromebooks para centros educativos de Google

Gracias a sus funciones de seguridad integradas y listas para usar, los ordenadores Chromebook son una solución muy segura, escalable e intuitiva para alumnos y docentes. Nunca se ha registrado un ataque de ransomware en ningún dispositivo ChromeOS empresarial, escolar o de consumo. Los Chromebooks contribuyen a proteger los centros educativos frente a nuevas amenazas gracias a funciones actualizadas. Además, las actualizaciones se aplican en segundo plano de forma automática para que los usuarios retomen su trabajo en cuestión de segundos.

Actualizaciones automáticas de SO y aplicaciones con protección integrada contra malware

Los atacantes están continuamente tratando de aprovechar los errores y carencias de los SOs, los navegadores y las aplicaciones populares para instalar malware y robar datos de usuarios. Para protegeros a ti y a tus usuarios, los Chromebooks mantienen el SO y las aplicaciones actualizados, puesto que tienen mecanismos de protección integrados con actualizaciones de seguridad. Además, las aplicaciones en la nube no requieren actualizaciones de software como las locales. El chip de seguridad diseñado por Google que contienen los Chromebooks contribuye a la seguridad de los dispositivos, protege la identidad de los usuarios y garantiza la integridad del sistema.

En los Chromebooks de tu flota se ejecutarán las actualizaciones más recientes de protección contra malware de forma automática. Los alumnos y los docentes están protegidos contra ciberataques gracias a las funciones de seguridad integradas, como el cifrado de datos, el inicio verificado, el entorno aislado y las actualizaciones automáticas. .

Datos de usuarios seguros

Cuando inicias sesión en un Chromebook con tu cuenta de Google, todos tus datos se almacenan en archivos cifrados. Así, ninguna otra persona que acceda al dispositivo podrá ver tus datos ni iniciar sesión en las aplicaciones con tu cuenta. Esta característica ofrece una forma muy fácil y segura de que los alumnos compartan los dispositivos de un aula y de que los centros reduzcan los costes informáticos totales. La Licencia de Chrome Education, que permite gestionar dispositivos, ofrece funciones de seguridad más avanzadas y una visibilidad mejorada.

Políticas de seguridad de dispositivos gestionados por usuarios remotos

LLos administradores de los centros educativos pueden configurar políticas de ChromeOS e instalar y actualizar aplicaciones de forma remota con la consola de administración de Google. Con solo hacer clic en un botón, un único administrador de TI puede actualizar las políticas y configuraciones de cientos de miles de Chromebooks en un momento.

De esta manera:

- Los alumnos solo pueden acceder al contenido y las aplicaciones que haya aprobado el centro educativo
- Todas las aplicaciones y extensiones se actualizan con las correcciones de seguridad más recientes
- Los usuarios no pueden copiar, transferir ni transmitir datos escolares a otro dispositivo
- Puedes tomar decisiones basadas en los datos con recomendaciones de seguridad personalizadas de Google para abordar las amenazas
- Puedes gestionar de forma centralizada las políticas de seguridad y de gestión de identidades y accesos para todos los usuarios en la propia consola de administración

Las siguientes son algunas políticas destacadas que los administradores quizás quieran configurar:

Políticas de dispositivos

- **Modo Invitado**
  Es recomendable inhabilitar el modo Invitado del dispositivo para que los alumnos y docentes tengan que iniciar sesión con sus credenciales en lugar de usar el dispositivo de forma anónima
- **Restrições de login**
  Puede que no quieras que los alumnos y docentes inicien sesión en los Chromebooks del centro educativo con sus cuentas de Gmail personales. En el caso de los dispositivos que usen únicamente los alumnos, implementa restricciones de inicio de sesión para que se limiten solo a tu dominio de Workspace.
- **Informes de usuarios y de dispositivos**
  Los administradores deben plantearse activar los informes de usuarios y de dispositivos para registrar con qué frecuencia se usan los Chromebooks, quién los usa y en qué condiciones se encuentra el hardware.
- **Obligación de volver a realizar el registro**
  Es vital que los Chromebooks que pertenecen a un centro educativo no salgan de él a menos que un administrador los dé de baja. Los administradores deberían contemplar la posibilidad de aplicar la política que obliga a volver a realizar el registro de los Chromebooks para que estos se registren de nuevo automáticamente si se borran sus datos o sufren un intento de robo.

Políticas de usuarios

- **Modo Incógnito**
  Los alumnos deben recibir los Chromebooks escolares listos para sacarles partido. Esto implica limitar los dispositivos para que solo puedan usar el navegador autenticado, cuyos filtros de contenido web evitarán que accedan a sitios web inadecuados. Los administradores deberían inhabilitar el modo Incógnito para que los alumnos no puedan eludir los filtros web.
- **Modo proxy**
  Aunque algunos centros educativos pueden usar proxies para filtrar el contenido web, es importante desactivar los ajustes que permiten que los usuarios puedan cambiar la configuración de proxy.
- **Acceso mediante inicio de sesión múltiple**
  Si se permite que los usuarios inicien sesión en una cuenta secundaria mientras usan Chromebooks o cuentas de Workspace del centro educativo, cabe la posibilidad de que un usuario utilice la cuenta secundaria para filtrar al exterior información o datos sensibles de los alumnos o el centro educativo fácilmente. Los administradores deberían plantearse bloquear el acceso mediante inicio de sesión múltiple.
- **Historial del navegador**
  En el caso de los alumnos, puede ser beneficioso inhabilitar las opciones que les permiten borrar el historial de navegación. Si se produjera un incidente de seguridad en Internet, los registros del historial podrían ser de ayuda durante su investigación.

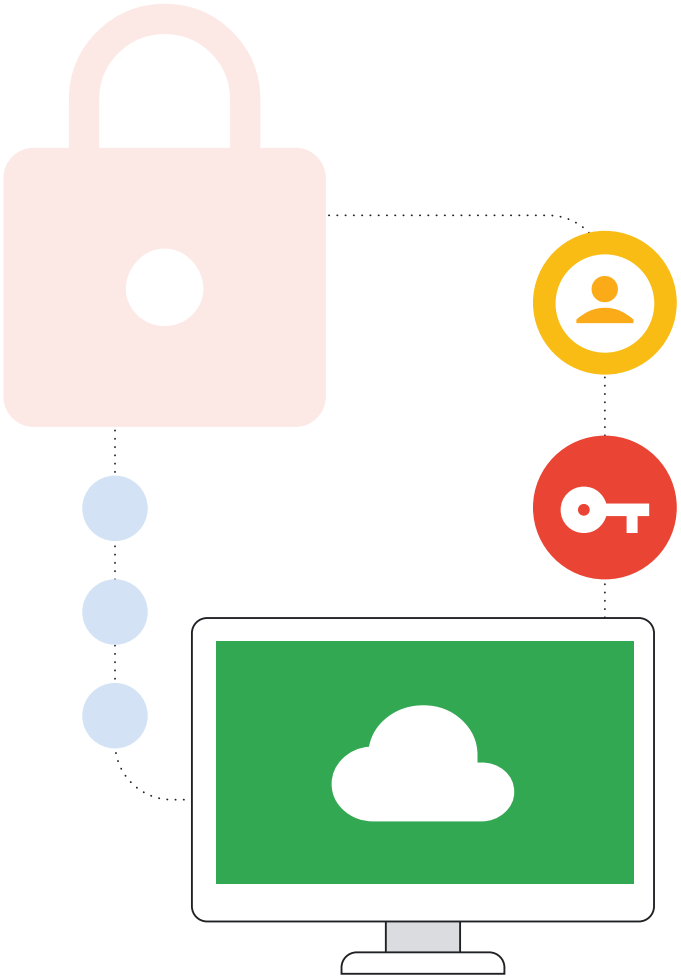
Esta lista es un buen punto de partida para proteger tus redes frente a los errores más típicos que derivan en incidentes cibernéticos de gravedad considerable. Puedes consultar nuestra lista de comprobación de seguridad para obtener información sobre otras políticas de seguridad recomendadas.

Uso seguro en cualquier momento y lugar mediante gestión de endpoints

El sistema de gestión remota de políticas que ofrece ChromeOS permite a los administradores de los centros educativos aplicar ajustes y ejecutar herramientas de seguridad, como sistemas de filtros de contenido, en los dispositivos, en lugar de hacerlo en los servidores de red del centro. Así, los alumnos pueden usar sus Chromebooks en casa y disfrutar de la misma protección que tienen en el aula. Este beneficio es cada vez más importante, ya que en los centros educativos cada vez se usan más libros de texto digitales y herramientas de aprendizaje online, con lo que los alumnos necesitan llevarse los ordenadores a casa para hacer los deberes.

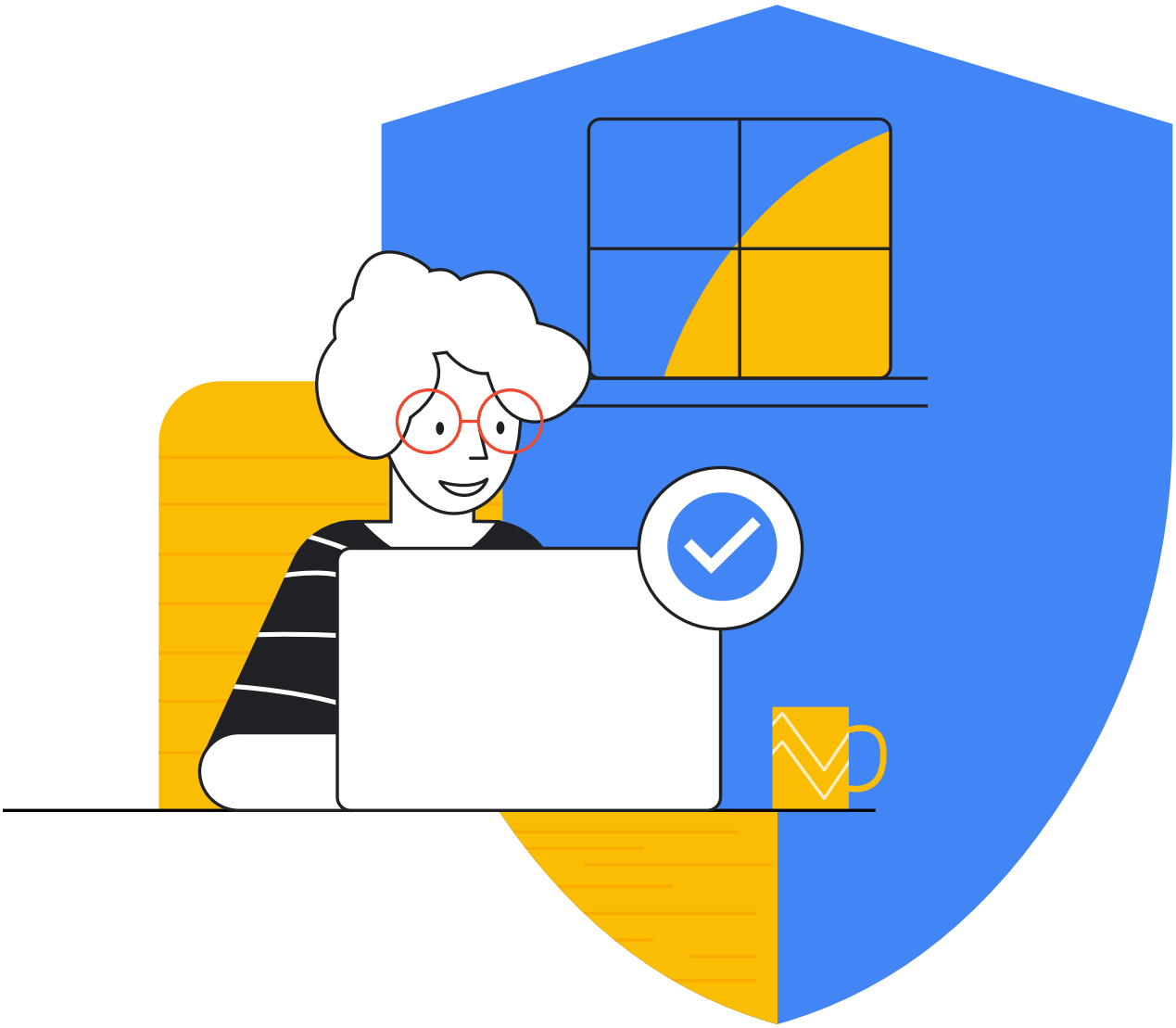
Conclusión

Abordar los retos que plantea la protección de las instituciones de enseñanza primaria y secundaria frente a los incidentes cibernéticos es una labor compleja, pero vale la pena invertir en tu seguridad y la de los alumnos, los docentes, el personal y el ecosistema online en general. Aunque las cuestiones que se abordan en este documento son un buen punto de partida, cada centro educativo tendrá que adaptar las recomendaciones a sus necesidades particulares, así como esforzarse por seguir el ritmo del panorama de amenazas en constante cambio y de las tecnologías emergentes. Esta guía, que permite sentar cimientos sólidos para programas de seguridad en el ámbito de la enseñanza primaria y secundaria, es un recurso que indica los pasos que puedes dar y medidas que se pueden tomar. Google también dispone de diversos recursos, formaciones y profesionales de la ciberseguridad cualificados que pueden ayudar a los centros educativos y las organizaciones que quieran aplicar esta guía, así como en materia de tecnologías emergentes como la IA. Los productos de Google diseñados para el ámbito educativo proporcionan soluciones listas para usar que abordan muchos de los problemas de ciberseguridad que se detallan en este documento. Nos encantaría colaborar contigo en el diseño y la implementación de tus programas de seguridad.



Lista de recursos

- Google. “Consejos de seguridad online”. Centro de Seguridad de Google, https://safety.google/security/security-tips/. Fecha de consulta: 6 de octubre del 2022.
- NIST. “Marco para la mejora de la seguridad cibernética en infraestructuras críticas, Versión 1.1”. Publicaciones NIST Technical Series, 16 de abril del 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Fecha de consulta: 6 de octubre del 2022.
- Microsoft. “Microsoft AccountGuard”. Programa Microsoft AccountGuard, https://www.microsoftaccountguard.com/es-es/. Fecha de consulta: 6 de octubre del 2022.
- Google. “Programa de Protección Avanzada”. Programa de Protección Avanzada de Google, https://landing.google.com/advancedprotection. Fecha de consulta: 6 de octubre del 2022.
- Google. “Centro de Seguridad de Google”. “Seguridad en Internet - Centro de Seguridad de Google”, https://safety.google. Fecha de consulta: 6 de octubre del 2022.
- Meta. “Aspectos básicos de Meta: Proteger tu cuenta”. Proteger tu cuenta, https://www.facebook.com/gpa/resources/basics/security. Fecha de consulta: 6 de octubre del 2022.
- Meta. “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect. Fecha de consulta: 6 de octubre del 2022.
- NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise”. Publicaciones NIST Technical Series, https://doi.org/10.6028/NIST.SP.800-124r1. Fecha de consulta: 6 de octubre del 2022.
- Llaves de acceso: https://developers.google.com/identity/passkeys
- Informe de CISA “Protecting Our Future” sobre ciberseguridad en la enseñanza primaria y secundaria: https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Informe de GAO: https://www.gao.gov/products/gao-20-644
- Para obtener más información sobre cómo puede ayudarte Google for Education a proteger tu institución, consulta el Centro de privacidad y seguridad de Google for Education.
- Informe de Zscaler sobre phishing



Google for Education