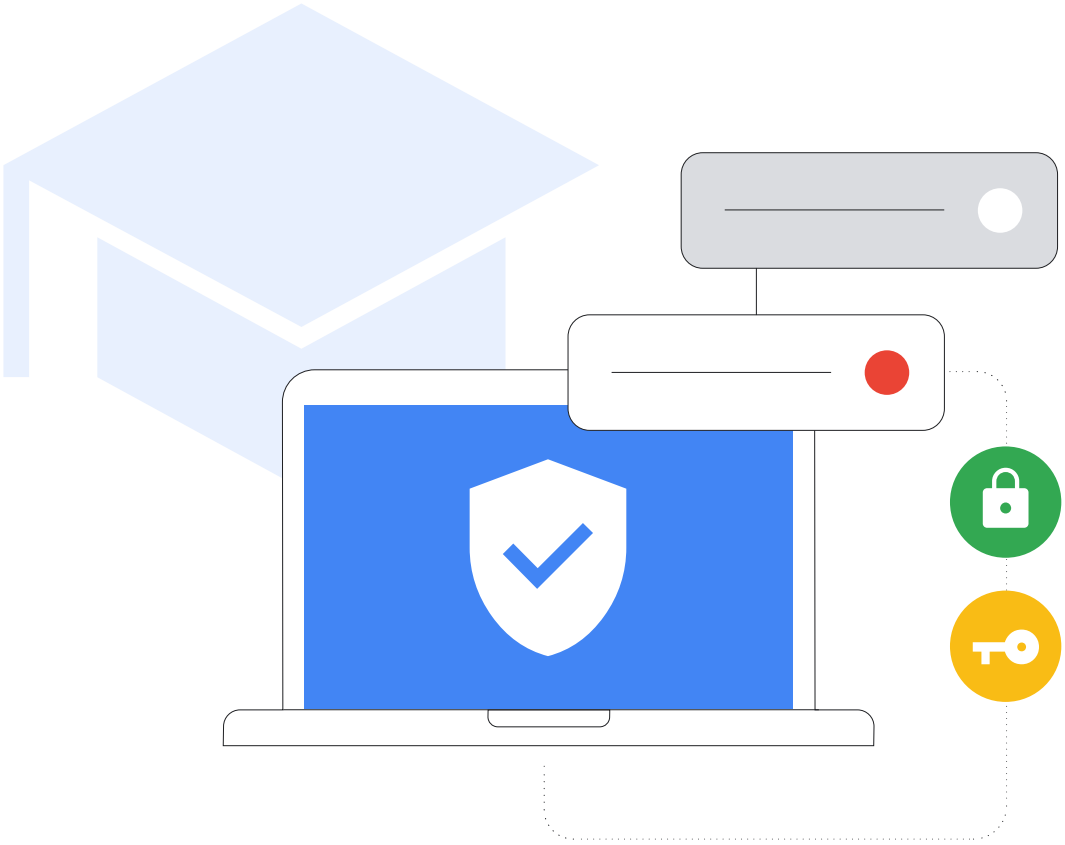
Google for Education

Actualización de agosto de 2023 de la guía de seguridad cibernética para los niveles de preescolar a bachillerato



Safer with Google

Resumen ejecutivo

Como se destaca en el informe Protecting Our Future[1] de la CISA, es fundamental que las instituciones de preescolar a bachillerato inviertan en seguridad cibernética para proteger a sus estudiantes, familias, profesores, personal y comunidades. En este documento, se proporcionan prácticas recomendadas y una orientación para los administradores de TI acerca de cómo configurar hardware y software en las instituciones de preescolar a bachillerato para reforzar la seguridad cibernética. El documento incluye prácticas recomendadas generales y orientación específica sobre los productos y servicios de Google. La misión de Google de organizar la información de todo el mundo y lograr que sea accesible y útil para todos es el motor fundamental del trabajo que realizamos en el equipo de Google for Education: crear herramientas diseñadas para la enseñanza y el aprendizaje. Compartiremos lecciones sobre ese trabajo en esta guía.

Contamos con prácticas recomendadas de seguridad por tema que ofrecen una visión más profunda sobre configuración y estrategias de mitigación de riesgos. También explicamos cómo Google aborda la seguridad cibernética en sus servicios, en especial las herramientas de educación. Si bien en este documento proporcionamos orientación detallada y válida para cualquier producto o servicio, creemos que nuestros productos ofrecen una protección superior contra los ataques comunes desde el primer momento.

El riesgo

Las instituciones educativas son los principales objetivos de los ciberataques, ya que las entidades que actúan de mala fe tratan de aprovecharse de los entornos escolares con gran cantidad de datos para beneficiarse. El 46% de las instituciones educativas que aún no han sido objeto de ataques cree que acabarán sufriéndolos, ya que los ataques de ransomware son cada vez más sofisticados y difíciles de detener. Y el 42% de estas instituciones considera que el ransomware es tan frecuente que ser víctima de ataques es inevitable. Cuando en el 2020 se debió pasar con rapidez al modelo de educación a distancia, surgieron muchas lagunas de seguridad cibernética que dejaron a las instituciones educativas vulnerables a los ataques.

La defensa

Estos ataques se pueden mitigar. Y aunque ninguna tecnología elimina por completo los riesgos, el sector de la educación y los proveedores de tecnología educativa pueden trabajar juntos para adoptar y aplicar prácticas recomendadas que permitan crear un enfoque integral y seguro que disminuya significativamente los riesgos. Cuando las instituciones educativas implementan las precauciones y políticas correctas para proteger a los usuarios, asegurar los dispositivos y garantizar la privacidad de los datos, pueden administrar mejor el riesgo y mitigar los ataques.

Recomendaciones clave:

- **USA AUTENTICACIÓN SEGURA** para proteger la información sensible, los correos electrónicos, los archivos y otros tipos de contenido, y evitar que los usuarios no autorizados accedan a los sistemas educativos. Implementa las prácticas recomendadas para la autenticación de usuarios, como contraseñas seguras y verificación en dos pasos (2SV), llaves de acceso y administradores de contraseñas cuando sea posible, especialmente en el caso de los administradores de TI y el personal que trabaja con información sensible.
- **APLICA UNA CONFIGURACIÓN DE SEGURIDAD ADECUADA** para mantener a salvo a los usuarios, los datos y el entorno. Aunque los productos de Google son seguros de forma predeterminada, es fundamental que los administradores también usen y configuren de forma adecuada las redes y los sistemas para garantizar la seguridad. Para proteger las instituciones educativas, aplica los principios de confianza cero y privilegio mínimo, es decir, los usuarios solo deben tener acceso al software, los datos, las aplicaciones y los sistemas que necesitan para hacer su trabajo de manera eficaz.
- **ACTUALIZA Y MEJORA TUS SISTEMAS** para asegurarte de que los usuarios estén protegidos de las amenazas más recientes. Usa sistemas operativos (SO) y navegadores modernos, y asegúrate de que todos los usuarios ejecuten las versiones de software más recientes en todos los dispositivos (o versiones estables a largo plazo aprobadas) y que se actualicen automáticamente. Cambiarse a una solución más segura, como las Chromebooks, puede aumentar la seguridad. Nunca se han detectado ataques de ransomware contra dispositivos ChromeOS.
- **USA SISTEMAS DE ALERTAS Y SUPERVISIÓN EN TIEMPO REAL** para mejorar tu postura de seguridad y mitigar posibles problemas con rapidez. Puedes usar estas funciones integradas en tu software de colaboración y comunicación principal, como Google Workspace for Education, o implementar soluciones independientes de registro y supervisión de seguridad. Asegúrate de realizar un seguimiento integral de las actividades en la red, los dispositivos, las aplicaciones, los usuarios y los datos de tu institución educativa. Vigila los accesos a las cuentas, el uso compartido de archivos, el volumen de correos electrónicos (en particular los que parezcan phishing y software malicioso), la actividad de los dispositivos y los cambios de configuración. Mantén actualizada tu solución de alerta y supervisión para recibir notificaciones sobre amenazas, eventos importantes y cambios en los sistemas.
- **CAPACITA A LOS PROFESORES, EL PERSONAL Y LOS ESTUDIANTES** para usar los dispositivos y el software de manera segura, reconocer e informar posibles amenazas, y compartir datos de forma adecuada. De esta forma, podrán protegerse de los ataques más comunes. Las instituciones o los distritos educativos pueden crear materiales de capacitación con su marca, además de usar materiales ya preparados y disponibles de manera gratuita, para ofrecer un kit de herramientas integral para las instituciones educativas.

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

Recomendaciones específicas para los usuarios de los productos de Google:

Los productos de Google como Google Workspace for Education y las Chromebooks pueden mejorar la seguridad cibernética de tu institución educativa y facilitar la implementación de cada una de estas recomendaciones. Juntos, proporcionan una solución integral que protege la privacidad de los usuarios y ofrece seguridad de primer nivel para tu institución.

Estas estrategias, junto con la orientación adicional que se proporciona en este documento, constituyen una base excelente para la seguridad de las instituciones de preescolar a bachillerato.

Enfoque de Google para la educación

La misión de Google es organizar la información de todo el planeta y lograr que sea accesible y útil para todos, incluido el sector de la educación. En el equipo de Google for Education, lo hacemos creando herramientas como Chromebooks y Google Classroom que hacen que sea sencillo y seguro para los estudiantes y profesores crear, compartir y organizar su contenido, y acceder y usar recursos educativos y herramientas en línea.

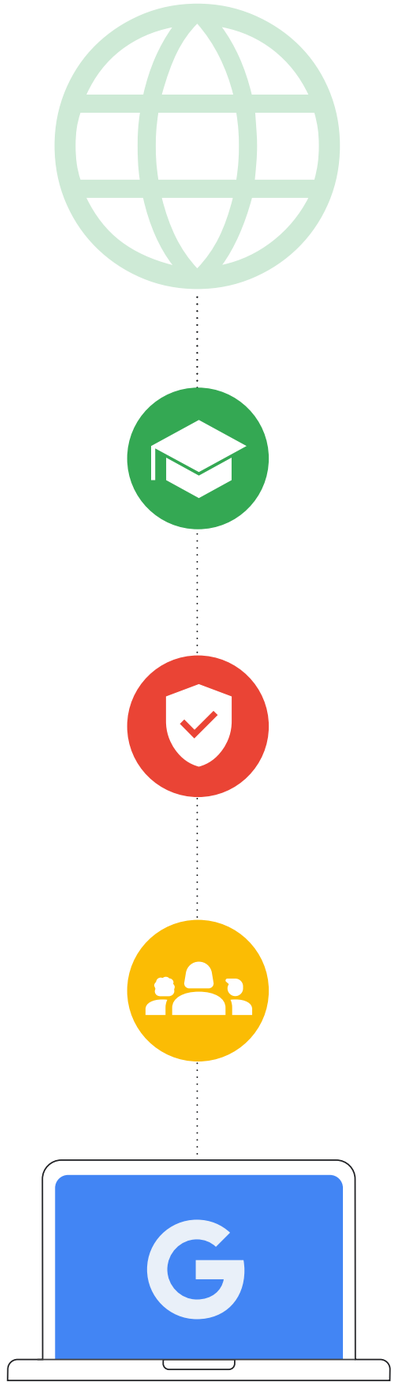
Las instituciones educativas merecen tecnología que sea segura de forma predeterminada, tenga diseño de privacidad integral, te permita mantener el control y tenga información y contenido confiables. Con productos como Chromebooks y Google Workspace for Education, las instituciones educativas obtienen seguridad de primer nivel que cumple con los más altos estándares educativos mundiales. Así, los administradores consiguen visibilidad

total y control de los datos y las políticas de seguridad sin complicaciones, y los estudiantes pueden sumergirse completamente en el proceso de aprendizaje dentro de un entorno digital seguro que incluye contenido apropiado para su edad y mitiga el spam y las amenazas cibernéticas.

Priorizamos las funciones y los controles de seguridad integrados, los estándares más altos de privacidad y las opciones de herramientas de seguridad más proactivas para garantizar un aprendizaje seguro para todo el mundo. Los dispositivos ChromeOS ayudan a mitigar las amenazas a las que se enfrentan las instituciones educativas y son la mejor defensa contra la amenaza número uno: el ransomware, ya que nunca se han producido ataques de ransomware exitosos contra Chromebooks.

Además, Google Workspace for Education es uno de los paquetes de comunicación y colaboración basado en la nube más popular y seguro del mundo. Para obtener más información sobre cómo cada uno protege la seguridad cibernética en relación con las recomendaciones que se incluyen aquí, consulta la última sección.

Este documento se divide en dos secciones: la primera incluye orientación práctica y general sobre seguridad para las instituciones de preescolar a bachillerato independientemente de los productos que usen, y la segunda contiene orientación específica de configuración para las instituciones que usan productos de Google for Education, como Google Workspace for Education y Chromebooks. En ambas secciones, se proporciona información para ayudar a que tú y tus estudiantes naveguen de forma segura en línea.



Introducción

Los dispositivos y las redes de las instituciones de preescolar a bachillerato corren un alto riesgo de sufrir ciberataques. Por lo tanto, es fundamental que usen la mejor seguridad posible para proteger a los estudiantes y evitar la pérdida de datos, servicios, recursos, tiempo y dinero que puede producirse debido a estos ataques (Fuente).

Esta guía es una herramienta para divulgar las prácticas recomendadas de seguridad cibernética que los administradores de las instituciones educativas y los sistemas escolares deben implementar para proteger mejor sus entornos. Si lo hacen, las instituciones de preescolar a bachillerato pueden mitigar o evitar ciberataques graves y costosos a los sistemas educativos además de proteger a los estudiantes, las familias, los profesores y el personal.

Los ciberataques dirigidos a las instituciones educativas son cada vez más frecuentes y graves. Según el K-12 Cybersecurity Resource Center, entre el 2016 y el 2021 se produjeron más de 1,300 incidentes cibernéticos divulgados públicamente y relacionados con organizaciones educativas en los 50 estados. Los líderes educativos actuales deben proteger los datos y la información personal de los estudiantes, los profesores y el personal, así como los sistemas y la información de sus instituciones. Es una tarea difícil, sobre todo si se tiene en cuenta que, tradicionalmente, el sector educativo ha tenido más dificultades para seguir el ritmo de los cambios en seguridad cibernética frente a otros sectores.

Los ciberataques exitosos, como ransomware, phishing, software malicioso y muchos otros más, pueden provocar violaciones de seguridad a gran escala de información de identificación personal (PII), pagos costosos (desde el 2020, el valor promedio de un rescate aumentó 5 veces, a USD 812,260) y causar interrupciones prolongadas de la enseñanza y otras operaciones de las instituciones educativas. Recientemente, un ataque de ransomware exitoso inhabilitó un sistema escolar completo, lo que provocó un efecto dominó en toda la comunidad, ya que los estudiantes no pudieron asistir a la institución educativa durante varios días. Si siguen teniendo recursos y fondos limitados, las organizaciones de preescolar a bachillerato seguirán siendo uno de los principales blancos de estos ataques, a menos que aumenten la inversión en seguridad cibernética.

La seguridad cibernética siempre es mejor si hay comunicación, colaboración y asociación. Este documento se creó a partir de las sugerencias de seguridad y protección de Google, el Marco de seguridad cibernética del National Institute for Standards and Technology (NIST) y el kit de herramientas y las recomendaciones del 2023 para seguridad cibernética en instituciones de preescolar a bachillerato de la CISA, que son fuentes de prácticas de seguridad cibernética ampliamente aceptadas. En el documento, también se analizan los pasos generales que los administradores de TI deben adoptar o considerar, algunas de las prácticas recomendadas de Google, la orientación para nuestros productos, y también hace referencia a las sugerencias de seguridad y los servicios que ofrecen otras empresas. Los administradores deben revisar toda la orientación de seguridad que ofrecen las empresas pertinentes y, además, implementar las recomendaciones más actuales, dado que las empresas responsables son las más capacitadas para describir sus productos y cualquier cambio que se haya producido en ellos.

Antes de llevar a la práctica las recomendaciones que figuran a continuación, también debes tener en cuenta los siguientes factores:

Consideraciones

1. **Protección para la población estudiantil.**

   Las necesidades de cada institución educativa son diferentes, y ciertas poblaciones pueden requerir medidas adicionales para proteger su seguridad y privacidad. Muchas herramientas de tecnología educativa tienen funciones que facilitan el acceso según la edad, como, por ejemplo, limitar el contenido inapropiado o garantizar la privacidad de los datos de ubicación y contacto.

2. **Los tipos de datos que almacenas.**

   Si almacenas datos sensibles, recomendamos que los encriptes o almacenes en una ubicación diferente.

3. **Los tipos de dispositivos que usas y tu modelo de implementación.**

   Los dispositivos y sus aplicaciones deben recibir actualizaciones automáticas para maximizar la seguridad, encriptar los datos y aislar las cuentas para garantizar que los usuarios solo tengan acceso a su propia información.

4. **Las políticas de tu institución educativa, distrito o región.**

   Es posible que tu institución educativa tenga políticas específicas con respecto al uso de tecnología. Deberás asegurarte de que todas las medidas de protección estén configuradas de acuerdo con estas políticas.

Todos los días, Gmail bloquea **100 millones** de intentos de phishing.

Cada semana, Google identifica **300,000** sitios web peligrosos.

Todos los días **74 millones** de usuarios reciben ayuda del Administrador de contraseñas de Google.

Cada año **700 millones** de personas están más protegidas con la Verificación de seguridad.

Recomendaciones generales sobre seguridad

Usa autenticación segura

La autenticación segura debe ser la prioridad principal de todas las instituciones, no solo las educativas. En el cuarto trimestre del 2022, las cuentas poco seguras o no acreditadas representaron el 48% de todos los factores de riesgo en las violaciones de seguridad. Implementa algunas recomendaciones clave para verificar que los usuarios sean quienes dicen ser y limitar el acceso a la información adecuada para cada rol de usuario.

Los administradores de TI deben aplicar de manera forzosa el uso de la verificación en dos pasos o 2SV (también conocida como autenticación de dos factores o 2FA) y pasar a la autenticación sin contraseñas (es decir, con llaves de acceso) siempre que accedan terceros de forma remota a los sistemas de la institución educativa. La 2SV agrega una capa de seguridad adicional a las cuentas en línea, lo que dificulta el acceso a los atacantes.

Existen muchos tipos de dispositivos y modelos de implementación que usan las instituciones educativas, y existen varios niveles de aptitud técnica en los entornos de preescolar a bachillerato. La seguridad de las cuentas y los dispositivos cambia según los roles y los tipos de usuario con determinadas prácticas recomendadas: los administradores de TI, los profesores y el personal, los estudiantes más grandes que usan dispositivos asignados y los estudiantes más jóvenes que usan dispositivos compartidos. Analizaremos las recomendaciones específicas para cada grupo a continuación.

Existen varios métodos de autenticación que son prácticas recomendadas en la mayoría de los entornos:

- **Contraseñas seguras**
  Se les pide a los usuarios que creen sus propias contraseñas la primera vez que acceden. Estas deben tener requisitos mínimos de complejidad y longitud. Las frases de contraseña más largas proporcionan más seguridad debido a su longitud y al uso de caracteres complejos. No se debe exigir a los usuarios que cambien regularmente sus contraseñas, ya que eso los alienta a usar opciones más sencillas o a realizar cambios irrelevantes (como actualizar un solo carácter).

- **Verificación en dos pasos (2SV)**
  La 2SV protege las cuentas con un segundo paso que, a menudo, requiere de un objeto que tiene el usuario, como una llave de seguridad o una app en su teléfono celular para crear un código de verificación único. Aunque cualquier forma de 2SV agrega seguridad a las cuentas, los administradores deben evitar el uso de códigos de verificación enviados por mensaje de texto o llamadas, ya que pueden ser vulnerables a ataques basados en números de teléfono.

- **Autenticación sin contraseña**
  Las llaves de acceso son una alternativa más segura y sencilla a las contraseñas. Los usuarios pueden acceder a las apps y los sitios web con un PIN, patrón, sensor biométrico (como una huella dactilar o reconocimiento facial), o bien presionando una llave de seguridad, lo que evita que tengan que recordar y administrar contraseñas. Aunque puede que estas opciones no sean adecuadas para todos los contextos educativos, reemplazan cada vez más a las formas tradicionales de autenticación y permiten accesos más seguros y rápidos. Las llaves de acceso protegen a los usuarios de los ataques de phishing, ya que solo funcionan en las apps y los sitios web registrados.

- **Inicio de sesión único (SSO)**
  El SSO permite a los usuarios acceder a múltiples aplicaciones y sitios web con un solo conjunto de credenciales. Cuando los usuarios solo deben recordar un conjunto de credenciales, es menos probable que las anoten. Además, cuando las instituciones educativas no tienen que administrar varios conjuntos de credenciales de usuarios, pueden ahorrar dinero en asistencia de TI y costos del departamento de ayuda. Google Workspace for Education admite el SSO de forma nativa, de manera que los usuarios puedan usar las credenciales de su Cuenta de Google para acceder a aplicaciones de terceros, o puedan usar las credenciales de otro proveedor para acceder a sus Cuentas de Google.

- **Administradores de contraseñas**
  Pueden ayudar a los usuarios a crear contraseñas únicas y seguras en las cuentas y los servicios que usan durante sus días de clase y laborales (cuando no usan el SSO). No permiten acceder al sistema operativo de un dispositivo, pero pueden administrar contraseñas una vez que el usuario se haya conectado. Los usuarios de Google pueden utilizar el administrador de contraseñas en Chrome en cualquier plataforma, como ChromeOS y Android..

Las necesidades específicas de diversos grupos se beneficiarán de subconjuntos especializados o combinaciones de estos enfoques de autenticación según su rol dentro de la institución educativa, el tipo de sistemas y datos a los que tienen acceso y su edad.

Administradores de instituciones educativas

Los administradores controlan los sistemas y gran parte de los datos de las instituciones de preescolar a bachillerato. La protección de sus cuentas es clave para la seguridad de todo el sistema: desde la infraestructura hasta los datos de las cuentas y los dispositivos que administra la institución. Por ello, deben adoptar el estándar de oro en materia de autenticación, que incluye el uso de contraseñas seguras, un administrador de contraseñas sólido y la 2SV. Cada una de estas opciones ofrece una capa de protección que, cuando se combinan, proporcionan la mayor seguridad para 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 solicitudes. Esto puede incluir 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 tienen un botón de encendido que se puede utilizar para llevar a cabo la autenticación de dos factores.
- Los administradores deben usar un administrador de contraseñas de confianza compatible con la 2SV para almacenar las contraseñas en servicios diferentes.

Profesores y personal que usan dispositivos asignados

Al igual que los administradores, los profesores y el personal tienen acceso a datos sensibles, pero no controlan la infraestructura digital y tienen niveles de aptitud técnica más variados.

- Los profesores y el personal que usan Chromebooks deben tener la opción de acceder con la verificación biométrica (por ejemplo, con una huella dactilar) cuando la ley lo permita.
- Los administradores deben aplicar de manera forzosa el uso de la 2SV y pasar a la autenticación sin contraseñas siempre que sea posible y cuando un miembro del personal acceda de forma remota a los sistemas de la institución educativa.

Estudiantes más grandes que usan dispositivos asignados
(por lo general, desde 4° grado)

Los estudiantes más grandes tienen más conocimientos sobre cómo protegerse y suelen ser capaces de usar mecanismos de autenticación más seguros, lo que resulta apropiado para los tipos de servicios que probablemente utilizarán. Solo deben tener acceso a su propia cuenta y a la información que se compartió con ellos.

- Los estudiantes que usan Chromebooks deben tener la opción de crear un PIN específico del dispositivo para poder acceder a él más rápido. Es posible que las opciones biométricas no sean adecuadas o viables en muchos entornos escolares.
- Se debe ayudar a cada estudiante a crear una contraseña única que no incluya información personal (p. ej., nombres, aulas o cumpleaños). Se debe enseñar a los estudiantes cómo el uso de frases de contraseña puede aportar complejidad y, a su vez, son fáciles de recordar.

Estudiantes jóvenes que usan dispositivos compartidos
(normalmente de preescolar a 3er grado)

Los estudiantes más jóvenes aún están aprendiendo a usar la tecnología educativa y se beneficiarán de la autenticación sencilla, que es adecuada para servicios y datos limitados.

- Las instituciones educativas que usen alternativas a las contraseñas de terceros (como códigos QR o acceso con imágenes) para los estudiantes más jóvenes y aquellos que no pueden acceder con contraseñas deben tomar precauciones en materia de seguridad, ya que son menos seguras. Los administradores deben modificar las contraseñas de los estudiantes y actualizar el código cada vez que se pierda un código o haya quedado expuesto a terceros.
- Las instituciones educativas deben educar a estudiantes, madres y padres sobre la importancia de mantener en secreto las contraseñas y almacenar de forma segura las credenciales alternativas, como los códigos QR.
- En el caso de los dispositivos asignados, como tablets, se puede usar un PIN específico del dispositivo como método alternativo de autenticación segura.

Aplica parámetros de configuración de seguridad adecuados

Los dispositivos y las redes escolares son un objetivo de gran visibilidad y valor para los atacantes de todo el mundo, por lo que es fundamental implementar la máxima seguridad posible para evitar la pérdida de servicios, recursos, tiempo y dinero. Los administradores del sistema deben implementar funciones de seguridad eficaces y adecuadas que estén disponibles en los productos que usan las instituciones, pero también deben asegurarse de que estos sistemas sigan siendo fáciles de usar para los profesores, el personal y los estudiantes. Los parámetros de configuración de seguridad y privacidad importantes deben configurarse de tal forma que los usuarios individuales no puedan inhabilitarlos o modificarlos, y otros parámetros de configuración deben tener los valores predeterminados de protección que establezca el administrador. Es fundamental implementar la máxima seguridad posible para evitar la pérdida de servicios, recursos, tiempo y dinero. Si usas Chromebooks, puedes consultar nuestras sugerencias para establecer políticas de dispositivo en la última sección.

Por último, incorpora la "minimización de datos" a tus prácticas. Para ello, limita los fines y medios de recopilación, uso y divulgación de la información personal de los individuos a lo que sea r

Aplicaciones y actualizacionesr

Limita y minimiza las apps que los usuarios pueden instalar, ya que cada aplicación instalada en un dispositivo es un posible vector de ataque que puede aprovecharse. Si es posible, usa aplicaciones de fuentes confiables. Por ejemplo, recomienda a los usuarios que busquen la insignia de verificación en Google Play Store para asegurarse de descargar aplicaciones oficiales que pasaron por una revisión de seguridad. Cualquier modificación del SO o hardware (otorgar permisos de administrador o liberarlos) introduce fallos de seguridad importantes y debe evitarse.

Acceso y visibilidad

Los administradores deben asegurarse de que los usuarios solo tengan acceso a los datos, el software, los servicios y los sistemas que necesitan para desempeñar sus funciones o aprender de manera eficaz. Esto limita el acceso no intencionado y permite realizar un seguimiento de quiénes accedieron a qué recursos. Presta especial atención a los datos altamente sensibles, como la PII de los usuarios, y a los sistemas (como RR.HH., nóminas, calificaciones, seguridad y configuración). Para ello, audita qué usuarios pueden acceder a los datos y en qué circunstancias, limita el acceso a los dispositivos que pertenecen a la escuela y asegúrate de que solo tengan acceso determinados miembros del personal.

Revisa las políticas de uso compartido de datos en las herramientas de colaboración para evitar el acceso inapropiado, la divulgación excesiva y el acceso no autorizado. Limita o bloquea el uso compartido fuera de tu entorno (especialmente para los estudiantes) y habilita políticas que supervisen el uso compartido de contenido sensible.

Pérdida o robo de dispositivos

Perder un dispositivo no tiene por qué implicar una pérdida de datos. Los administradores deben crear un plan estándar para garantizar el acceso a la información y los documentos en caso de que se pierdan dispositivos o los roben, como el mantenimiento de documentos en un entorno en la nube. Descarga e imprime códigos de respaldo de tus procesos de 2SV para evitar que se interrumpa el acceso a las cuentas.

Cuando se informe el robo o extravío de un dispositivo, asegúrate de que este pueda bloquearse de forma remota (si es posible) y de que las cuentas asociadas estén bloqueadas o marcadas para garantizar que no se usen para obtener acceso no autorizado. Las Chromebooks pueden limpiarse de manera remota si se pierden, y las cuentas de Google Workspace for Education pueden supervisarse para detectar actividad sospechosa o suspenderse (bloquearse) si es necesario.

Protección avanzada para los usuarios de alto riesgo

En el caso de los usuarios que tienen información sensible y alta visibilidad (como los administradores de Google Workspace for Education), Google ofrece el Programa de Protección Avanzada (APP). El APP les brinda a los usuarios protección adicional contra los ataques dirigidos, como intentos de phishing, descargas dañinas y violaciones de contraseñas. El APP se diseñó específicamente para frustrar los ataques dirigidos en línea a las Cuentas de Google y utiliza de forma automática autenticación sólida y llaves de seguridad, además de restringir el acceso de terceros a datos de las cuentas. Otros proveedores de cuentas en línea también ofrecen protecciones de cuentas sólidas para los usuarios de alto riesgo, y los administradores y el personal siempre deben usarlas si tienen acceso a información personal o sistemas de tecnología.

Actualiza y mejora tus sistemas

Una de las consideraciones más importantes que cualquier persona puede tener para protegerse es mantener actualizados el sistema operativo y las aplicaciones. Esto es aún más importante para las instituciones de preescolar a bachillerato, ya que son una parte muy importante de la educación de los niños y de sus vidas cotidianas. La mayoría de los ataques de software malicioso en contextos educativos y en otros contextos de alto riesgo se basaron en Windows, como SolarWinds, el ataque de ransomware al Distrito Escolar Unificado de Los Ángeles, el hackeo del Distrito Escolar de Little Rock, la violación de la seguridad de los datos de Microsoft Exchange Server, el ataque de ransomware del Distrito Escolar de Albuquerque, y la reciente violación de datos de agencias federales de Microsoft. Este es otro punto en el que el uso de productos y servicios en la nube debería facilitar las tareas de los administradores, ya que así se reduciría la superficie de ataque y se garantizaría que los sistemas y las aplicaciones se mantengan actualizados automáticamente.

Cámbiate a un sistema operativo moderno y mantenlo actualizado

La versión más reciente de cualquier sistema operativo (SO) suele contener funciones de seguridad nuevas para prevenir los vectores de ataque conocidos. Debes habilitar la funcionalidad de actualización automática en el SO del dispositivo o, si no es posible, descarga e instala parches y actualizaciones de un proveedor de confianza al menos una vez por mes.

Las Chromebooks funcionan con ChromeOS, por lo que tienen actualizaciones automáticas frecuentes con los parches de seguridad más recientes para permitir la adopción rápida de las innovaciones de seguridad más actuales y verifican la integridad del sistema operativo de solo lectura antes de iniciarse. También encriptan todos los datos almacenados en el dispositivo, lo que lo protege del acceso no autorizado y permite ejecutar cada página web y aplicación en una zona de pruebas independiente, por lo que si un sitio web o una app se infectan con software malicioso, este no podrá propagarse a otras partes del dispositivo.

Si tu institución educativa no está lista para cambiarse a las Chromebooks, ChromeOS Flex es una versión de ChromeOS diseñada para modernizar los dispositivos de tu institución. ChromeOS Flex proporciona a todos una experiencia de enseñanza y aprendizaje unificada y moderna, que cuenta con funciones proactivas de administración basada en la nube y seguridad integrada. Flex puede brindar protección automatizada y bloquear apps y ejecutables maliciosos sin reemplazar el hardware existente.

Usa un navegador actualizado y mantenlo al día

Es importante garantizar que el navegador también esté actualizado y sea seguro. Los navegadores actualizados ofrecen funciones de seguridad más avanzadas y pueden pedirles a los usuarios que las habiliten fácilmente o posibilitar que los administradores las configuren para activarlas de forma predeterminada en las computadoras institucionales. Esto les permite proteger la confidencialidad de la información sensible en tránsito por Internet. Los navegadores deben mantenerse actualizados. Ya sea para trabajar, aprender o realizar otra actividad en línea, un navegador actualizado podrá realizar las siguientes acciones:

- **Utilizar una seguridad fuerte**, como el aislamiento de sitios y la protección de navegación segura para evitar que los usuarios ingresen accidentalmente en sitios web peligrosos
- **Habilitar actualizaciones automáticas** para garantizar que el navegador reciba actualizaciones de seguridad rápidamente.
- **Garantizar que la conexión sea segura.** Los navegadores actualizados deben usar seguridad de la capa de transporte, y los usuarios pueden hacer clic junto a las URLs y verificar que la conexión esté marcada como segura

Chrome se diseñó para ofrecer seguridad y cuenta con funciones como la Navegación segura activada de forma predeterminada. Y existe un administrador de contraseñas integrado que puede autocompletar contraseñas a medida que navegas por la Web, lo que te permite usar contraseñas seguras de forma sencilla.

Usa sistemas de alertas y supervisión en tiempo real

Los sistemas de alertas y supervisión en tiempo real pueden ayudar a las instituciones educativas a identificar las amenazas y reaccionar ante ellas rápidamente, antes de que puedan causar daños. Es importante asegurarse de que las herramientas de seguridad se ejecuten en segundo plano, recopilando y registrando eventos de seguridad de todos los sistemas. Las herramientas de IA son especialmente útiles para analizar grandes cantidades de datos recopilados y encontrar anomalías y patrones, que podrían utilizarse para detectar más rápido y fácilmente las amenazas y poder procesar y abordar las vulnerabilidades. Esto permite priorizar las actividades que debe revisar el administrador o el personal de TI.

Las instituciones educativas pueden usar las funciones de alertas y supervisión integradas en el software principal de colaboración y comunicación, como Google Workspace for Education, o implementar soluciones independientes de gestión de eventos e información de seguridad (SIEM).

Los sistemas de alertas y supervisión en tiempo real pueden hacer un seguimiento de distintas actividades en la red, los dispositivos, las aplicaciones, los usuarios y los datos de una institución educativa, como los accesos de usuario, el acceso a archivos, posibles intrusiones, robos o intentos de robos de datos y actividades del administrador.

Si el sistema detecta alguna actividad sospechosa, puede enviar una alerta al personal de TI de la institución educativa. Esto permite a los administradores investigar el problema y tomar medidas para mitigar la amenaza.

Además, las herramientas de alertas y supervisión pueden usarse para comprender mejor las amenazas que enfrentan las instituciones educativas. A través del análisis en tiempo real de los datos de estos sistemas, las instituciones educativas pueden identificar tendencias y patrones que pueden ayudarles a protegerse mejor.

Aquí encontrarás algunas de las prácticas recomendadas para usar los sistemas de alertas y supervisión (incluidos los de SIEM):

1. **Define tus objetivos de seguridad**
   Identifica qué información y sistemas son los más importantes para la institución educativa, y qué tipos de amenazas presentan el mayor riesgo para ellos. Luego, identifica los datos que debes recopilar para supervisar esas amenazas.

2. **Recopila los datos correctos y configura de forma apropiada**
   Es importante recopilar los datos correctos y configurar las aplicaciones para abordar los objetivos de seguridad más relevantes. Esto puede incluir datos de firewalls, filtros de contenido, sistemas de detección de intrusiones, servidores web y otros dispositivos de seguridad, además de software de comunicación y colaboración, sistemas de información escolar y sistemas de gestión de aprendizaje.

3. **Investiga las alertas y responde a ellas**
   Cuando tu sistema de supervisión genera una alerta, es importante investigar el problema y adoptar las medidas adecuadas. Esto puede implicar reunir a varios equipos para investigar el origen de la alerta, determinar si es un falso positivo o adoptar los pasos para mitigar la amenaza, como suspender cuentas, restablecer contraseñas de usuarios, poner en cuarentena o borrar correos electrónicos, cambiar permisos de archivo o limpiar dispositivos.

Capacita a los profesores, el personal y los estudiantes

Las instituciones de preescolar a bachillerato deben promover la conciencia y los hábitos de seguridad en sus comunidades a través de campañas y asociaciones que empoderen a los usuarios. Es fundamental educar a los profesores, el personal y los estudiantes sobre la importancia de la seguridad para ayudarlos a protegerse en línea y a evitar amenazas graves de seguridad cibernética. Enséñales cómo usar los productos y servicios implementados en la institución, cómo detectar e informar amenazas como correos electrónicos de phishing y, lo más importante, cómo adoptar medidas para evitar estos ataques. Las instituciones educativas y los distritos deben promover la conciencia y los hábitos de seguridad en sus comunidades a través de campañas y asociaciones que empoderen a los usuarios.

Cómo usar dispositivos y software de manera segura

Los administradores pueden asociarse con profesores y expertos para desarrollar planes de estudios sobre seguridad cibernética adecuados para la edad que ayuden a los estudiantes a entender cómo usar dispositivos, software y sistemas de forma segura. Crear materiales de capacitación con la marca de la institución educativa o el distrito ayuda a contextualizar las recomendaciones para profesores y estudiantes, pero también puedes aprovechar el material prediseñado disponible, como Sé genial en Internet en Safety.Google y Khan Academy, y adaptarlo a tus necesidades. Estos programas pueden ayudar a los usuarios a protegerse sin importar dónde estén, ya sea en la institución educativa o en la comunidad.

Reconoce las amenazas

Capacitar a los profesores, el personal y los estudiantes para reconocer las amenazas es fundamental para su seguridad. Es importante enseñarles a los niños cómo saber si algo es una amenaza o no, ya que tal vez no sepan cómo distinguir si el contenido es legítimo. Hay algunos tipos de amenazas que deben reconocer y saber cómo denunciar, y los administradores deben centrarse en esos temas que consideran que tendrán los mayores beneficios. Lo más importante es que la capacitación no solo debe enseñarles a los usuarios a reconocer las amenazas, sino también a adoptar medidas contra ellas. Las amenazas comunes que los usuarios deben reconocer incluyen ransomware, phishing, ingeniería social, software malicioso y estafas, pero si ciertas amenazas son más frecuentes en una institución determinada, es buena idea asegurarse de que la comunidad educativa reciba capacitación sobre ellas.

Uso compartido seguro de datos y archivos

Se debe capacitar a los profesores y al personal sobre el uso compartido adecuado de archivos y datos y cómo reconocer solicitudes inadecuadas a través de correo electrónico. Lo más importante es que deben asegurarse de que la información personal sensible solo se comparta o procese cuando sea necesario y con capas adicionales de protección, por ejemplo, que nunca se comparta por correo electrónico o con terceros. Deben usar funciones de prevención de 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 seguridad social) o copien y peguen contenido sensible fuera del dominio.

El enfoque de Google en acción: dispositivos y servicios para la educación

La adquisición de software es una de las herramientas más poderosas que un distrito escolar tiene para protegerse. El software debe tener una arquitectura y un diseño sólidos para minimizar el riesgo de vulnerabilidades, con seguridad integrada en cada capa. Cuando se solicita a las instituciones educativas que compren software seguro o software de empresas con una trayectoria de seguridad comprobada, los riesgos cibernéticos generales pueden reducirse significativamente. Por ejemplo, en Google reforzamos nuestro ChromeOS y seguimos implementado soluciones más inteligentes y proactivas que aprovechan la solidez de nuestra experiencia en aprendizaje automático, identidad y la nube.

En Google, estamos comprometidos a crear productos que protejan la privacidad de estudiantes y profesores, y que le brinden a tu institución seguridad de vanguardia. Puedes confiar en que los productos y servicios de Google for Education protegen continuamente a los usuarios, los dispositivos y los datos frente a amenazas cada vez más complejas. En esta sección, se explican a los administradores de TI las recomendaciones de seguridad cuando usan productos de Google for Education.

Google Workspace for Education

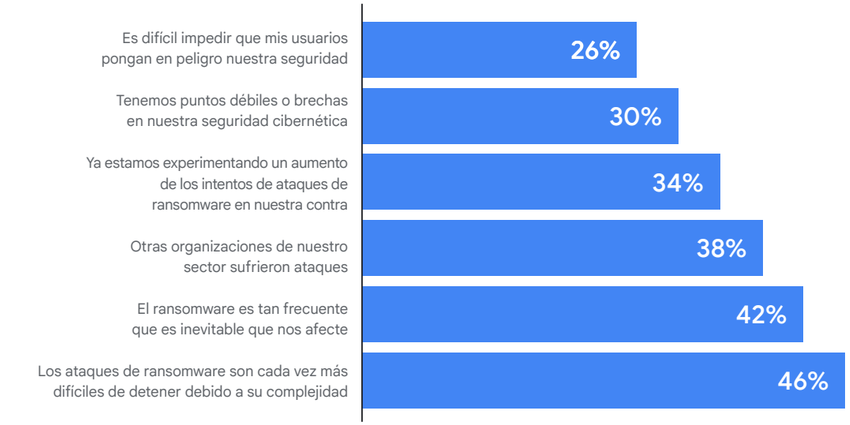
Google Workspace for Education es un conjunto de herramientas y servicios de Google que se diseñaron para colaborar, optimizar la enseñanza y proteger el entorno de aprendizaje de las instituciones educativas. Los productos y servicios de Google for Education protegen continuamente a los usuarios, los dispositivos y los datos frente a amenazas cada vez más complejas, y proporcionan herramientas, como centros de alerta y seguridad, bóveda de detección electrónica, administración de identidades y accesos, y prevención de pérdida de datos.

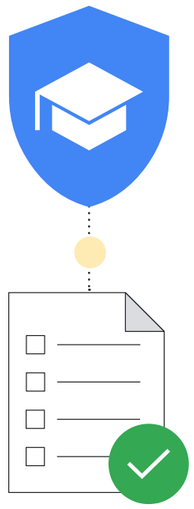
Si estás empezando a usar Google Workspace for Education, tenemos materiales útiles para ti. Muchos de ellos pueden ayudarte a configurar productos de acuerdo con las recomendaciones mencionadas en esta orientación. Si quieres obtener ayuda para comenzar con Google Workspace for Education, consulta esta Guía de inicio rápido y configuración para TI.

Lista de tareas de seguridad

Revisa las listas de tareas de seguridad y obtén más información para fortalecer la seguridad y privacidad de tu institución. Las instituciones educativas que usan las ediciones Standard y Plus de Google Workspace for Education también pueden consultar la página Estado de seguridad para supervisar la configuración de los parámetros de la Consola del administrador. Por ejemplo, puedes verificar el estado de los parámetros de configuración como el reenvío automático de correo electrónico, la encriptación del dispositivo, la configuración de uso compartido de Drive y mucho más. Si es necesario, puedes realizar ajustes en la configuración de tu dominio según los lineamientos generales de seguridad y las prácticas recomendadas, a la vez que alineas estas pautas con las necesidades comerciales y la política de administración de riesgos de tu organización.

Por qué se prevé un golpe para el sector educativo





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

Aquí encontrarás algunas sugerencias útiles para asegurarte de estar aprovechando al máximo las protecciones incorporadas en Google Workspace for Education:

Configura unidades organizativas (UO)

Es indiscutible que todos en tu cuenta de Google Workspace for Education deben tener la misma configuración. Las unidades organizativas son grupos de usuarios que te permiten otorgar diferentes servicios, parámetros de configuración y permisos a distintos usuarios. Por ejemplo, con 2SV para los profesores y el personal, y autenticación adecuada para la edad para los estudiantes jóvenes. Configura unidades organizativas diferentes para el personal, los profesores y los estudiantes para aplicar políticas a cada grupo de usuarios por separado. Una estructura bien diseñada es fundamental para administrar de forma eficaz y flexible tu cuenta de Google Workspace for Education..

Configura políticas de contraseñas y protecciones de cuentas de administrador

Como dijimos, la autenticación de usuarios es fundamental para mantener tu institución protegida. Por ello, configuramos maneras flexibles de gestionar la autenticación para administradores, que te permitirán garantizar que los usuarios tengan las protecciones adecuadas y seguras para las cuentas. Establece políticas de contraseñas para garantizar que los usuarios creen contraseñas seguras, y considera solicitar el uso de 2SV cuando sea apropiado según los grupos recomendados en la sección Acceso seguro. Puedes aplicar el uso de 2SV para un subconjunto de usuarios (y darles tiempo para configurarlo) y, además, implementar 2SV utilizando una variedad de métodos, como llaves de seguridad (máxima protección), mensajes de Google (con apps de Google en iOS y Android), generadores de apps de verificación (como Autenticador de Google), y mensajes de texto o llamadas telefónicas (aunque estos son el método menos seguro).

Si tu organización usa un proveedor de identidad (IdP) distinto de Google, puedes configurar el inicio de sesión único (SSO) a través de un proveedor de identidad externo. Y, si lo prefieres, puedes usar la 2SV con SSO para las cuentas que no sean de administrador avanzado.

Activa o desactiva servicios

Los administradores pueden controlar a qué servicios de Google pueden acceder los usuarios con sus cuentas de Google Workspace for Education en la Consola del administrador de Google. Puedes controlar el acceso a los servicios de Google, como Calendario, Drive y Meet, activando o desactivando los servicios por unidad organizativa (UO). También puedes activar los servicios cuando uses grupos. Además, puedes revisar las diferencias entre los servicios principales y adicionales de Workspace antes de habilitar servicios adicionales como YouTube, Google Maps y Blogger. Se recomienda a los administradores que establezcan el acceso a los servicios de Google según la edad y que tengan en cuenta que los usuarios designados como menores de 18 años tienen restricciones automáticas en algunos servicios de Google cuando ingresan a sus cuentas de Google Workspace for Education.

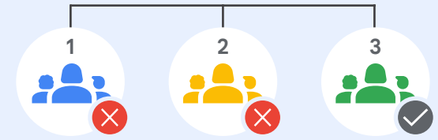
También puedes usar el acceso adaptado al contexto (disponible en Workspace for Education Standard y Plus) para permitir o bloquear el acceso a las apps de Google, como Gmail, Drive y Calendario, según la dirección IP, el origen geográfico, las políticas de seguridad o el SO de un dispositivo. Por ejemplo, puedes permitir Drive para computadoras solo en dispositivos de la empresa en países o regiones específicas.

Métodos para darles a los usuarios acceso a los servicios

En la Consola del administrador 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 usar Drive, tienes 2 opciones:

1. Mover a los usuarios a una unidad organizativa que tenga activado el acceso a Drive.
2. Agregar 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 tiene el servicio desactivado.

Unidades organizativas



Google Drive está desactivado para las unidades organizativas 1 y 2

En un grupo de acceso

Pero 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

Establece políticas de uso compartido de datos y reglas de retención

Como administrador, puedes controlar si los usuarios pueden compartir archivos y carpetas de Google Drive con personas fuera de la organización. Esto puede evitar que se compartan datos y archivos a personas que no correspondan o que se haga por error, lo que evita la filtración de datos. Separar los archivos y las unidades, crear unidades organizativas y aplicar el principio de privilegio mínimo son factores importantes para evitar que los atacantes se desplacen por las redes si se infiltran en una cuenta. Cuantos menos datos y acceso a la red tenga un posible atacante, menor es el daño que puede hacer.

Desactiva el uso compartido externo de archivos para los estudiantes (o restríngelo solo a los dominios permitidos) y establece el "Verificador de acceso" en "Solo con los destinatarios". Si permites que algunos usuarios o todos compartan archivos fuera del dominio, activa una advertencia cuando lo hagan. Además, inhabilita la publicación de archivos en la Web y solicita a los colaboradores externos que accedan con una Cuenta de Google.

Asimismo, los clientes de Workspace for Education Standard y Plus pueden tener usuarios objetivo y reglas de confianza para establecer recomendaciones y restricciones de uso compartido más detalladas. Por ejemplo, con los usuarios objetivo, configuras el público predeterminado de uso compartido de vínculos para los profesores en "profesores y personal", en lugar de todas las personas en la institución. Con las reglas de confianza, puedes impedir que los estudiantes de primaria compartan archivos con estudiantes más grandes.

Revisa las políticas de unidades compartidas para garantizar que solo los usuarios adecuados puedan crear unidades compartidas y evitar que los usuarios externos accedan a ellas. Se recomienda que habilites solo a los administradores (o al personal y los profesores) a crear unidades compartidas y que administres su acceso con mucha atención.

Considera limitar la visibilidad del directorio y el uso compartido de contactos cuando sea posible. Puedes hacerlo inhabilitando el uso compartido de contactos para algunos usuarios o todos, o creando directorios personalizados para limitar qué usuarios son visibles para quién.

Configura las políticas de prevención de pérdida de datos (DLP) en Drive y Gmail para detectar y bloquear información sensible. Hay políticas prediseñadas que puedes usar para proteger información sensible común (como números bancarios o de tarjetas de crédito). También puedes crear políticas personalizadas en función de palabras clave, listas de palabras y expresiones regulares (regex).

Administra la configuración de Gmail

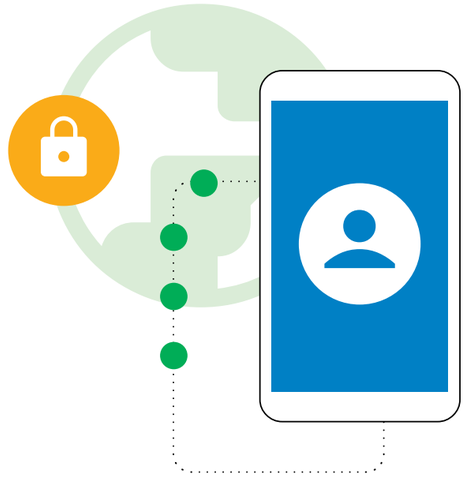
Gmail es uno de los servicios principales de Google Workspace for Education. Tiene muchos parámetros de configuración que los administradores pueden aprovechar para proteger a su institución y sus usuarios. Evita el spam, la falsificación de identidad y el phishing con la autenticación de Gmail. Personaliza la configuración del filtro de spam, lo que incluye solicitar la autenticación del remitente para todos los remitentes aprobados y, además, inhabilitar la omisión de los filtros de spam para los remitentes internos.

Inhabilita el acceso de POP/IMAP cuando sea posible y habilita el análisis mejorado de los mensajes previo a la entrega y la protección avanzada contra phishing y software malicioso. Si permites correos electrónicos externos para algunos de los usuarios o todos, puedes habilitar las advertencias de destinatarios externos.

Los clientes de Google Workspace for Education Standard y Plus también pueden protegerse contra el software malicioso y el ransomware a través de la configuración de reglas para detectar archivos adjuntos dañinos con la Zona de pruebas de seguridad.

Aplicaciones de terceros

Usa los flujos de trabajo de aprobación integrados para aprobar aplicaciones de terceros que accedan a los datos de la cuenta a través de APIs. Esto impide que los datos no autorizados se compartan con aplicaciones de terceros que no están aprobadas para el uso escolar.



Informes y supervisión

Como administrador, puedes consultar informes y registrar eventos en la Consola del administrador de Google para revisar la actividad en tu organización, como posibles riesgos de seguridad, ver quién accede y cuándo, y entender cómo los usuarios crean y comparten contenido. Puedes obtener datos a nivel de dominio junto con información más detallada a nivel de usuario a través de gráficos y tablas. Consulta informes y registros de auditoría (incluido el Centro de alertas) para identificar riesgos de seguridad, analizar el uso del servicio, diagnosticar problemas de configuración, hacer un seguimiento de la actividad de los usuarios y mucho más.

Los administradores de Google Workspace for Education Standard y Plus pueden aprovechar el panel de seguridad para ver una descripción general de diferentes informes de seguridad, identificar tendencias y comparar datos históricos y actuales, como el uso compartido de archivos en Drive, la actividad de spam, phishing y software malicioso en Gmail, los accesos sospechosos a cuentas de usuarios y las actividades sospechosas de los dispositivos. La mayoría de los registros de uso, actividad y auditoría (incluidos los eventos de registro de administrador, Drive, Meet y Chat) y los informes de seguridad están disponibles durante seis meses.

Aprovecha el centro de seguridad

Los administradores de Google Workspace for Education Plus y Standard pueden usar el centro de seguridad, que proporciona información y estadísticas de seguridad avanzados, así como mayor visibilidad y control de 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 y priorizar los problemas de seguridad y privacidad, como ataques de phishing, uso compartido de archivos inadecuado, actividad sospechosa de usuarios y dispositivos, etc., y tomar medidas sobre ellos.

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

0

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

50%

Un 50% de posibles ahorros en primas de seguro de seguridad cibernética gracias a Workspace

2x menos

incidentes de seguridad para organizaciones que usan Workspace en comparación con Microsoft 365

2.5x menos

incidentes de seguridad para organizaciones que usan Workspace en comparación con Microsoft Exchange

* Según la CISA, esta cifra es significativamente inferior a la de otros proveedores de productividad en este espacio.

Google Chromebooks for Education

Las Chromebooks son computadoras altamente seguras, escalables y fáciles de usar para estudiantes y profesores, gracias a sus funciones de seguridad integradas y listas para usar. Nunca se han informado ataques de ransomware exitosos contra dispositivos ChromeOS de empresas, instituciones educativas o usuarios particulares. Las Chromebooks ayudan a proteger a las instituciones educativas de las amenazas cambiantes con funciones actualizadas, y las actualizaciones se realizan automáticamente en segundo plano para que los usuarios puedan volver al trabajo en segundos.

Actualizaciones automáticas de SO y aplicaciones con protección integrada contra software malicioso

Los atacantes intentan constantemente aprovecharse de errores y brechas en los sistemas operativos, los navegadores y las apps populares para instalar software malicioso y robar datos de los usuarios. Para protegerte a ti y a tus usuarios, las Chromebooks mantienen actualizados el SO y las aplicaciones, ya que están diseñadas para brindar protección de forma predeterminada con actualizaciones de seguridad, y las aplicaciones en la nube nunca necesitan actualizaciones de software como las apps locales. Además, el chip de seguridad diseñado por Google que usan las Chromebooks protege los dispositivos y la identidad de los usuarios, y garantiza la integridad del sistema.

Las Chromebooks de tu flota ejecutarán automáticamente las actualizaciones más recientes de protección contra software malicioso. Los estudiantes y los educadores están protegidos de las amenazas cibernéticas con funciones de seguridad integradas, como encriptación de datos, inicio verificado, zonas de pruebas y actualizaciones automáticas.

Protege los datos de los usuarios

Cuando accedes a una Chromebook con tu Cuenta de Google, todos los datos se almacenan en archivos encriptados, lo que garantiza que nadie más en el dispositivo pueda ver tus datos ni acceder a aplicaciones con tu cuenta. Esto hace que sea muy fácil y seguro para los estudiantes compartir dispositivos dentro del aula y para las instituciones educativas reducir el costo informático total. Si buscas funciones de seguridad más avanzadas, la actualización de Chrome Education y la licencia de administración de dispositivos ofrecen visibilidad mejorada.

Políticas de seguridad configuradas de forma remota para los dispositivos administrados de los usuarios

Los administradores de las instituciones educativas pueden configurar las políticas de ChromeOS y, además, instalar o actualizar aplicaciones de forma remota con la Consola del administrador de Google. Con solo hacer clic en un botón, un único administrador de TI puede actualizar las políticas y los parámetros de configuración de cientos de miles de Chromebooks en unos minutos.

Esto garantiza lo siguiente

- Los estudiantes solo pueden acceder al contenido y a las aplicaciones que apruebe la institución educativa.
- Todas las aplicaciones y extensiones se actualizan con las correcciones de seguridad más recientes.
- Los usuarios no pueden copiar, transferir ni compartir datos escolares fuera del dispositivo.
- Se toman decisiones basadas en datos con las recomendaciones de seguridad personalizadas de Google para abordar amenazas de seguridad.
- Administración central de las políticas de seguridad y administración de identidades y accesos para todos los usuarios en la Consola del administrador.

Estas son algunas políticas destacadas que los administradores pueden configurar:

Políticas de dispositivo

- **Modo de invitado**
  Los Se recomienda que inhabilites el Modo de invitado de tus dispositivos para que los estudiantes y los profesores deban acceder con sus credenciales en lugar de usar el dispositivo de forma anónima.
- **Restricciones de acceso**
  No se recomienda que los estudiantes y profesores accedan a las Chromebooks de la institución educativa con sus cuentas de Gmail personales. Aplica restricciones de acceso que se limiten a tu dominio de Workspace solo para los dispositivos que utilizan exclusivamente los estudiantes.
- **Informes de usuarios y dispositivos**
  Los administradores deben considerar la posibilidad de activar los informes de usuarios y dispositivos para recopilar métricas sobre la frecuencia de uso de las Chromebooks, quiénes las usan y el estado del hardware.
- **Reinscripción forzada**
  Es fundamental que las Chromebooks que pertenecen a una institución educativa permanezcan en ella, a menos que un administrador las retire. Los administradores deben habilitar la reinscripción forzada de las Chromebooks para que estas siempre se reinscriban por sí mismas en caso de que se limpien o alguien las intente robar.

Políticas de usuario

- **Modo Incógnito**
  Los estudiantes deben recibir las Chromebooks de la institución educativa con la configuración correcta para poder usarlas. Esto incluye limitarlos a que usen el navegador autenticado para que los filtros de contenido web puedan mantenerlos alejados de los sitios web inadecuados. Los administradores deben inhabilitar el modo Incógnito para que los estudiantes no puedan eludir los filtros web.
- **Modo de proxy**
  Si bien algunas instituciones educativas pueden usar proxies para el filtrado web, es importante desactivar la posibilidad de que los usuarios cambien la configuración de proxy por su cuenta.
- **Acceso múltiple**
  Si los usuarios tienen permitido acceder a una cuenta secundaria cuando usan las Chromebooks y las cuentas de Workspace de la institución educativa, es posible que otros usuarios puedan transferir fácilmente datos o información sensible de los estudiantes o la institución educativa a esa cuenta secundaria. Los administradores deben considerar la posibilidad de bloquear el acceso múltiple.
- **Historial de navegación**
  Puede ser beneficioso inhabilitar la posibilidad de que los estudiantes borren el historial de navegación. Si ocurriera un incidente de seguridad de Internet, los registros del historial de Internet podrían ser beneficiosos durante la investigación..

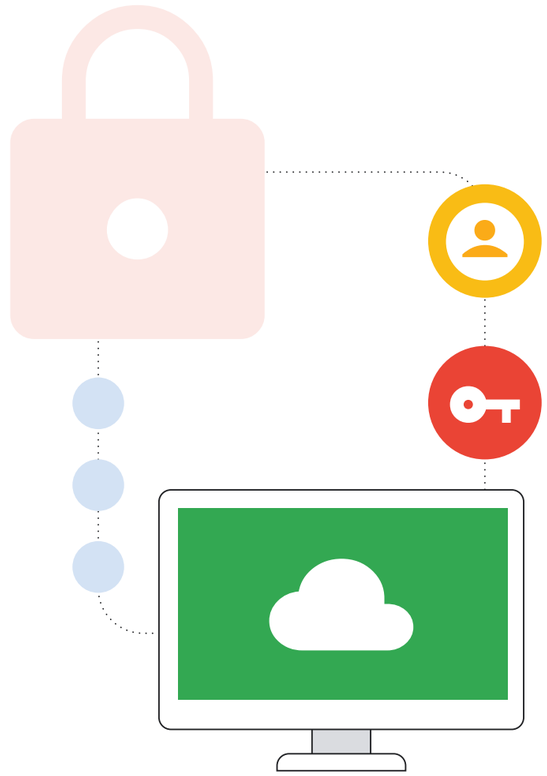
Esta lista es un buen punto de partida para garantizar que tus redes estén protegidas de los tipos de errores más comunes que provocan incidentes cibernéticos significativos. Puedes encontrar otras políticas de seguridad recomendadas en Lista de tareas de seguridad.

Administración de extremos para un uso seguro en cualquier momento y lugar

El sistema de administración remota de políticas de ChromeOS permite a los administradores de las instituciones educativas aplicar una configuración de seguridad y ejecutar herramientas de seguridad, como sistemas de filtrado de contenido en el dispositivo, en lugar de los servidores de red de la institución educativa. Esto garantiza que los estudiantes disfruten los mismos beneficios de seguridad de las Chromebooks de la institución educativa en casa y en el aula. Esta funcionalidad es cada vez más importante, ya que las instituciones educativas están migrando al uso de libros de texto digitales y herramientas de aprendizaje en línea, y necesitan enviar las computadoras a casa con los estudiantes para que hagan las actividades para el hogar..

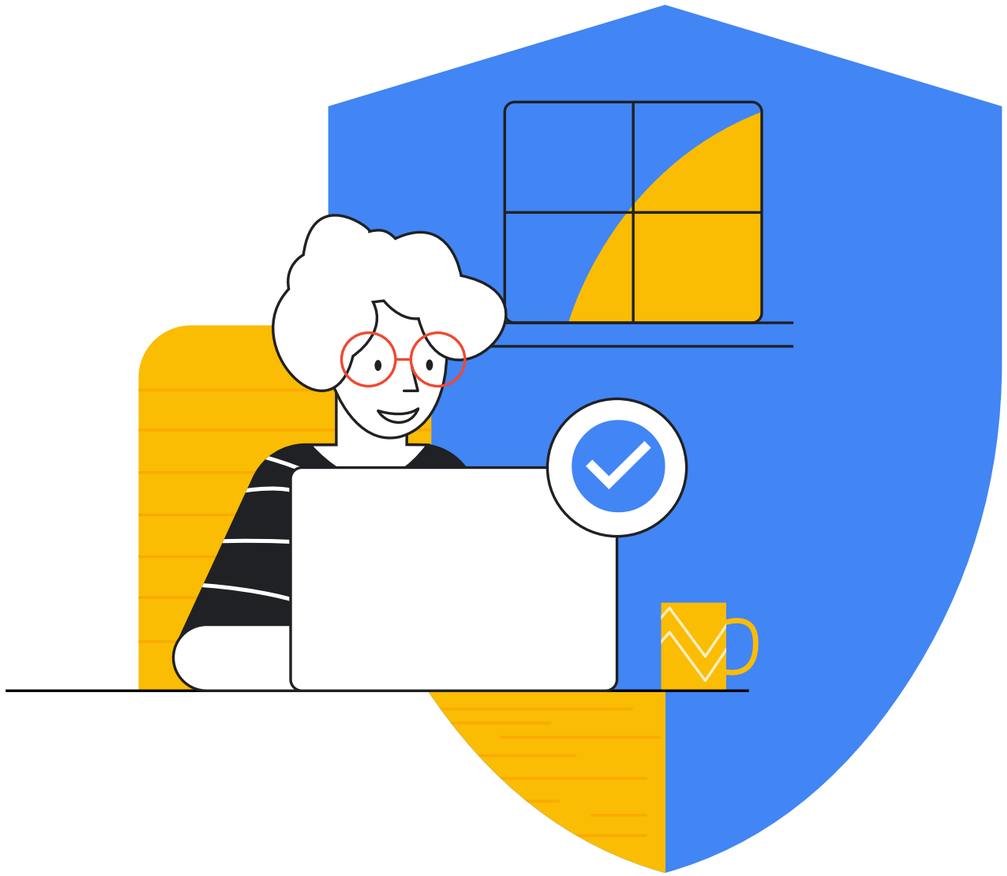
Conclusión

Los desafíos de proteger a las instituciones de preescolar a bachillerato contra los incidentes cibernéticos son complejos, pero vale la pena realizar la inversión y las tareas necesarias para protegerte a ti, los estudiantes, los profesores, el personal y el ecosistema en línea en su conjunto. Los temas que analizamos en este documento son un buen comienzo, pero cada institución educativa debe adaptar las recomendaciones en función de sus necesidades únicas y seguir el ritmo de la evolución de las amenazas y las tecnologías emergentes. Este recurso constituye una base sólida para cualquier programa de seguridad de preescolar a bachillerato y proporciona un modelo de referencia para los posibles próximos pasos y los elementos de acción implementables. Google también cuenta con una variedad de recursos, capacitaciones y profesionales calificados en seguridad cibernética para ayudar a las instituciones educativas y las organizaciones a seguir esta guía y enseñarles sobre tecnologías emergentes como la IA. Los productos de Google para la educación ofrecen soluciones prediseñadas para muchos de los problemas de seguridad cibernética que se indicaron en este documento. Estamos ansiosos por trabajar contigo cuando diseñes e implementes tus programas de seguridad..



Lista de recursos

- [1]Google. “Sugerencias para protegerte en línea”. Centro de seguridad de Google, https://safety.google/security/security-tips/. Fecha de acceso: 6 de octubre de 2022.
- [2]NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”. NIST Technical Series Publications, 16 de abril de 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Fecha de acceso: 6 de octubre de 2022.
- [3]Microsoft. “Programa Microsoft AccountGuard”. Programa Microsoft AccountGuard, https://www.microsoftaccountguard.com/en-us/. Fecha de acceso: 6 de octubre de 2022.
- [4]Google. “Programa de Protección Avanzada”. Programa de Protección Avanzada de Google, https://landing.google.com/advancedprotection. Fecha de acceso: 6 de octubre de 2022.
- [5]Google. “Centro de seguridad de Google”. Centro de seguridad de Google - Mejora tu protección en línea, https://safety.google. Fecha de acceso: 6 de octubre de 2022.
- [6]Meta. “Aspectos básicos: Protege tu cuenta”. Protege tu cuenta, https://www.facebook.com/gpa/resources/basics/security. Fecha de acceso: 6 de octubre de 2022.
- [7]Meta. “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect. Fecha de acceso: 6 de octubre de 2022.
- [8]NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise”. NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Fecha de acceso: 6 de octubre de 2022.
- Llaves de acceso: https://developers.google.com/identity/passkeys
- Informe Protecting Our Future sobre seguridad cibernética de preescolar a bachillerato de la CISA https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Informe de la GAO https://www.gao.gov/products/gao-20-644
- Para obtener más información sobre cómo Google for Education puede ayudarte a proteger tu institución, visita el Centro de seguridad y privacidad de Google for Education.
- Informe sobre phishing de Zscaler



Google for Education

Safer with Google