



GUÍA DEL MAESTRO DE escuela sabática para niños y jóvenes



safetysabbath.org



03 **Cómo utilizar esta guía**

04–05 **Hablar con nuestros niños sobre la seguridad en línea**

06 **Peligros comunes en internet**

- Seguridad de contraseñas
 - Perfil falso
 - Proteja su privacidad
 - Identificación de estafas
 - Otras cuestiones de seguridad
 - Acoso cibernético
-

12–14 **Actividad de los niños – Peligros comunes en internet**

15–16 **Preguntas para el debate**



Cómo utilizar esta guía

Este año para Safety Sabbath, Adventist Risk Management, Inc. (ARM) anima a las iglesias a mejorar su seguridad en línea y de redes. Parte del énfasis consiste en garantizar que los miembros tengan la educación y las herramientas necesarias para protegerse en línea. A menudo, una violación de la seguridad se debe a que los usuarios no practicaron seguridad en línea.

Esta guía para el maestro de la escuela sabática es una recopilación de recursos que usted puede utilizar para abordar el tema de la seguridad en línea con los niños y jóvenes que conoce. El objetivo de la primera sección, *Hablar con los niños sobre seguridad en línea*, es ayudarlo/a a entender cómo debe abordar este tema como maestro/a. El resto del documento contiene recursos que puede usar con sus clases de la escuela sabática, desde el nivel primario hasta el secundario.

Debido a que los jóvenes pasan mucho tiempo en línea, es cada vez más importante identificar y evitar los riesgos comunes. Mantener estas conversaciones con los niños y jóvenes es crítico, pero no piense que esas conversaciones tendrán lugar en el hogar o en la escuela. Y aunque así sea, insista en la importancia de practicar seguridad en línea a cada momento.

La sección *Peligros comunes en internet* está escrita para niños y jóvenes. Puede imprimir esta sección como un recurso para que ellos se lleven a casa. Quizá los niños más pequeños disfruten de la actividad, como una manera de reforzar los peligros de los que usted habla. Al mismo tiempo, los jóvenes mayores podrán aprovechar más las preguntas de debate que se incluyen.

El apóstol Pablo nos brindó una guía útil, que puede aplicarse a nuestro uso de internet. En Filipenses 4:8, dijo: «Por último, hermanos, consideren bien todo lo verdadero, todo lo respetable, todo lo justo, todo lo puro, todo lo amable, todo lo digno de admiración, en fin, todo lo que sea excelente o merezca elogio».¹

¹Biblica, Inc. (2011). La Santa Biblia. Nueva Versión Internacional



Hablar con los niños y jóvenes sobre la seguridad en línea

Los padres, maestros y líderes juveniles comprenden la necesidad de hablar con niños y jóvenes sobre los posibles peligros en línea. Sin embargo, esas conversaciones no suceden tan a menudo como debieran, y cuando ocurren, suelen fracasar en cuanto a marcar un cambio mensurable. Aprender a hablar con los niños y jóvenes sobre el poder de las redes sociales e internet puede dar a los adultos la confianza y los recursos necesarios para mantener esta conversación tan importante.

Educarse a sí mismos

Los cambios en internet se producen a la velocidad del rayo, y a menudo los padres y adultos quedan a oscuras en lo que se refiere a entender los peligros de internet. Antes de poder entablar una conversación significativa, los adultos deben invertir en educarse a sí mismos en lo que se refiere al panorama digital.

Saber cómo usan internet las personas jóvenes ofrece a los adultos la oportunidad de encauzar la conversación hacia los temas más pertinentes. De esta manera los adultos adquieren más credibilidad frente a los jóvenes, y es más probable que estos tomen con seriedad el consejo que les dan los adultos.

Las siguientes son algunas de las áreas en las que los padres y adultos deben estar actualizados:

- **Jerga de texto:** se ha desarrollado todo un nuevo lenguaje de abreviaturas y jerga en el espacio digital. Es importante saber qué dicen realmente los niños cuando se monitorean sus comunicaciones en línea.
- **Redes sociales:** familiarícese con las plataformas de redes sociales actualmente populares entre los jóvenes. Cree una cuenta y dedique tiempo a la aplicación para entender cómo se usa.
- **Juegos en línea:** los juegos en línea se han vuelto cada vez más sociales en años recientes. Muchos juegos populares están diseñados para grupos de personas conectadas en línea, e incluso para hablar mientras se juega. Sepa cuál es el último juego que hace furor, cómo se juega y si existe riesgo de cruzarse con desconocidos.

Concéntrese en los desafíos reales

Cuando hable con los jóvenes sobre internet, resista a la

Peligros comunes en internet

Año tras año, internet se integra cada vez más en todos los aspectos de la vida. No existe duda de que puede ser un recurso valioso, además de una excelente fuente de entretenimiento. Aun así, la internet no está exenta de riesgos potenciales que podrían ponerlo en peligro.

El noticiario a menudo informa sobre historias de jóvenes que conocen a una persona por internet y desaparecen después de intentar encontrarse con su nuevo «amigo». Es posible que usted diga: «Yo jamás haría eso», y quizá tenga razón. Sin embargo, existen muchos otros peligros en línea que tienen graves consecuencias.

Debido a que el mundo digital está tan interconectado, su seguridad en línea en realidad afecta a sus amigos, a su familia, a su iglesia y a su escuela. En general, cualquier persona con la que usted interactúa en línea también puede correr riesgo debido a las actividades que usted realiza en línea.

Considere esta posibilidad: piratean su correo electrónico, y de este modo el pirata informático puede enviar software malintencionado (denominado malware). Como el correo electrónico en apariencia proviene de usted, es más probable que sus amigos lo abran y hagan clic en el enlace. Si esto sucede en su escuela, a partir de ese momento la red de la escuela y todos sus usuarios están en riesgo. Vea lo rápido que estos hechos pueden ir aumentando hasta salirse de control.

Los piratas informáticos crean constantemente nuevos planes para engañarlo. Estos son algunos de los métodos más comunes que utilizan. Mientras repasa los peligros potenciales, piense si usted propició alguno de ellos. ¿Con qué facilidad caería usted en alguna de estas trampas si estuviera expuesto a ellas?



Seguridad de contraseñas

Su contraseña es lo único que lo separa a usted de un pirata informático. Si alguien puede ingresar en su correo electrónico, en sus redes sociales o en otras cuentas en línea, puede «convertirse» en usted. Eso puede darle al pirata informático más capacidad para ingresar en otras cuentas suyas o para hacerse pasar por usted cuando perpetre otros ataques.

En su contraseña, evite usar palabras o números que sean importantes para usted. Es verdad, de ese modo es más fácil de recordar. Sin embargo, el pirata informático también puede usar información recopilada de su perfil de redes sociales para intentar averiguar su contraseña. Sus equipos deportivos favoritos, fechas de cumpleaños y nombres de mascotas nunca deberían formar parte de sus contraseñas.

Al crear una contraseña, los expertos recomiendan usar una combinación de letras mayúsculas y minúsculas, números y símbolos especiales. Las contraseñas más largas son mejores, y no debería usar nunca una contraseña de menos de ocho (8) caracteres.

Si tiene una sola contraseña para todas sus cuentas en línea, aunque sea segura, estará en riesgo. Las contraseñas que pueden vulnerarse a menudo se venden entre los piratas informáticos, o se comparten en la «web oscura». Si usa la misma contraseña para varias cuentas, una contraseña vulnerada otorga acceso a todas sus cuentas.

La mejor manera para asegurarse de que los protocolos de las contraseñas sean buenos es utilizar una aplicación de gestión de contraseñas. Muchas de estas aplicaciones completan automáticamente su información de cada cuenta, es decir que usted puede usar contraseñas largas, especiales y seguras para cada una. Asegúrese de proteger su aplicación de gestión de contraseñas con una contraseña segura que no utilice en ningún otro lado. Podría considerar el uso de la denominada frase secreta para proteger su aplicación de gestión de contraseñas. Una frase u oración de varias palabras puede ser fácil de recordar, pero difícil de vulnerar.

En resumen: todo lo que usted haga en línea depende de lo seguras que sean sus contraseñas. Utilice contraseñas exclusivas para cada sitio, y jamás comparta su contraseña con nadie.



Catfishing

Quizá durante su infancia le enseñaron que las personas desconocidas eran peligrosas. Desde que éramos niños nos inculcaron esa idea y, como consecuencia, a menudo somos celosos de las personas a las que no conocemos. Con nuestros amigos o personas conocidas, es fácil bajar la guardia. Nos sentimos seguros, así que compartimos más cosas que con un desconocido.

Sin embargo, ¿conoce usted personalmente a todas las personas que lo siguen en las redes sociales? Y ¿cómo sabe que la persona con la que está interactuando en línea es quien dice ser?

La verdad es que no lo sabe. «Perfil falso» es el término utilizado cuando alguien crea una identidad falsa y detallada para fingir ser otra persona. A menudo el propósito es manipular a otros.

Muchas personas, incluidos los adultos, han sido engañadas con estafas de perfil falso. En el mejor de los casos, se sentirá avergonzado al darse cuenta de que lo engañaron para que creyera que su «amigo» en línea era alguien que no era. A menudo hay circunstancias peores, en las que la víctima sufrió estafa, chantaje, intimidación o abuso, emocional e incluso físico.

Los siguientes son algunos consejos para verificar si el perfil en línea de una persona coincide con su identidad:

- **Haga una búsqueda de su nombre:** si alguien usa su nombre completo en su perfil en línea, búsquelo en Google u otro motor de búsqueda. Si encuentra a la misma persona en diferentes plataformas de redes sociales, es una buena señal. También puede usar otros términos de búsqueda, como su domicilio o el nombre de su escuela, para acotar la búsqueda.
- **Búsqueda por imágenes:** En images.google.com, puede realizar una búsqueda por imágenes para saber dónde aparece esa imagen en internet. Haga clic en el ícono de la cámara en la barra de búsqueda de Google y escriba la dirección URL de la imagen, o cargue el archivo de la imagen. Suponga que su imagen de perfil proviene de un sitio de imágenes de archivo o se utiliza en varias cuentas diferentes de redes sociales (todas con otros nombres). En ese caso, es posible que la persona no sea quien dice ser.

Si sospecha que alguien no es quien dice ser, ¡bloquéelo de inmediato! De este modo cortará el acceso que esa persona tiene a su información.



Proteja su privacidad

El objetivo de las redes sociales es solo ese: social. Por estar conectados con amigos, es fácil publicar en línea más información de la que deberíamos. Es un problema, especialmente si no tenemos la configuración de privacidad apropiada en nuestras cuentas. Sin embargo, como aprendimos con los perfiles falsos, también puede ser un problema si somos «amigos» de personas a quienes no conocemos.

Comience verificando la configuración de privacidad y seguridad de todas sus cuentas de redes sociales e internet. Asegúrese de que sus fotos, videos, publicaciones y otros datos personales solo sean visibles para sus contactos. Muchos servicios le permiten establecer la configuración de privacidad como un valor predeterminado global. Sin embargo, debe investigar qué sucede con todas las publicaciones que hizo antes de cambiar su configuración de privacidad predeterminada.

Mientras verifica su configuración, asegúrese también de revisar la configuración de servicios de localización. Estos son útiles en aplicaciones y sitios web para saber dónde está localizado, para hacer sugerencias u ofrecer servicios de acuerdo con su ubicación. Sin embargo, esos sitios también pueden subir sus datos a internet: dónde vive, a qué escuela asiste o dónde pasa el rato.

Desactive los servicios de localización para las aplicaciones, y luego evalúe cada aplicación o sitio web que pide su permiso para usar servicios de localización. Si para usted esta funcionalidad es

absolutamente necesaria, solo dé permiso para seguir su ubicación en el momento de usar la aplicación. De este modo evita que la aplicación siga sus movimientos cuando no está abierta.

No dé más información que la necesaria en las redes sociales u otras cuentas en línea. Todo lo que usted comparte en el paisaje digital puede usarse para crear un perfil sobre usted. Piense con cuidado en los memes, bromas y opiniones que comparte en línea. Internet no olvida y, más adelante, esa broma o ese video de TikTok aparentemente inocente podría impedirle conseguir su empleo soñado.

La mejor regla general es suponer que todo lo que publica en internet es información pública y que cualquiera puede verla. La configuración de privacidad quizá ayude, pero es realmente necesario detenerse a pensar antes de cada publicación y de cada comentario que se comparte, se aprueba o se sigue.



Identificación de estafas

Las estafas por internet están en todas partes. El informe anual 2019 del Centro de Denuncias de Delitos en Internet del FBI mostró que la agencia tuvo un promedio de 1200 quejas por día, y muchas más que no fueron denunciadas. Las pérdidas para las víctimas en 2019 superaron los USD 3500 millones. Aunque es más probable que las personas ancianas sean víctimas de estas estafas, el informe IC3 mostró más de 55 000 casos denunciados por personas de menos de 30 años; las pérdidas por estos casos alcanzaron los USD 596,2 millones solo en 2019.²

Saber cómo identificar un engaño es un paso fundamental para no caer en la trampa de los estafadores. Las siguientes son algunas maneras de «detectar la estafa».

- ¡Si es demasiado bueno para ser verdad, probablemente lo sea! No es cierto que vaya a recibir el dispositivo más nuevo, zapatos de última moda o auriculares con un cincuenta por ciento de descuento.
- Si se trata de dinero, sea desconfiado. Esto incluye a las personas que quieren darle dinero a cambio de que usted les proporcione su número de cuenta bancaria. Incluso las solicitudes de dinero de personas que usted conoce deben verificarse; por ejemplo, la suma que piden y cuál es la mejor manera de enviarla.
- Antes de hacer clic en cualquier enlace incluido en correos electrónicos, mensajes de texto o publicaciones en las redes sociales, verifique quién envió el enlace y si este es legítimo. Pase el cursor sobre los enlaces antes de hacer clic sobre ellos para ver adónde lo llevarán en realidad. Si no está seguro sobre un enlace, no haga clic. Intente encontrar el sitio utilizando un motor de búsqueda para ver si las direcciones URL coinciden.
- A menudo los estafadores usan el miedo o la urgencia para hacer que la gente actúe sin tomarse tiempo para pensar. Los mensajes en los que insisten en que responda de inmediato

²Buró Federal de Investigaciones, Centro de Denuncias de Delitos en Internet. (2019). *Informe de Delitos en Internet 2019*. Extraído del sitio web IC3 del FBI: <https://www.ic3.gov/Home/AnnualReports>

suelen ser estafas, especialmente si parecen provenir de organismos con nombres oficiales como la Administración del Seguro Social. (No, nadie cancelará su número de seguro social).

- Conozca la dirección URL de la empresa con la que está interactuando, y verifique que se encuentra en el sitio correcto. A menudo, los estafadores compran nombres de dominio o direcciones URL similares que con frecuencia se escriben mal, en especial si lo hace desde su teléfono celular.

Otras cuestiones de seguridad

Estos son algunos otros consejos que lo ayudarán a estar seguro en línea:

- Si usa una computadora pública, como por ejemplo la de la biblioteca o la escuela, no permita que la computadora guarde su nombre de usuario o su contraseña. Cierre sesión en la computadora cuando termine, para borrar la caché y eliminar los archivos temporales a los que quizá haya tenido acceso.
- Las unidades externas pueden contener virus y malware. No use una unidad USB que haya encontrado en el suelo. Si no tiene antivirus en su computadora, tampoco debería usar la unidad externa de un amigo.
- Sea cuidadoso con las estaciones públicas de carga USB. Estas también pueden contener virus que podrían infectar su teléfono o computadora. En lugares públicos siempre es mejor cargar sus dispositivos con un cargador eléctrico que con un cable USB.

Acoso cibernético

El acoso cibernético es uno de los mayores desafíos a los que están expuestos los niños y adolescentes en internet. Muchas personas que nunca serían bravuconas en la vida real se vuelven más atrevidas cuando están escondidas detrás de la pantalla de una computadora, especialmente si creen ser anónimas.



Los Centros para el Control y la Prevención de Enfermedades (CDC) de Estados Unidos definen la intimidación como «un comportamiento agresivo indeseado por parte de otro joven o grupo de jóvenes... que implica un desequilibrio de poder observado o percibido, y se repite muchas veces o es muy probable que se repita». Observe que la intimidación no tiene que implicar violencia física, ni siquiera abuso verbal. Esparcir rumores acerca de una persona, publicar fotos degradantes o dejar intencionalmente a una persona fuera del grupo pueden ser acciones que se ajustan a la definición de intimidación. Los CDC manifiestan que 1 de 6 alumnos en la escuela secundaria informa haber sido víctima de intimidación en línea.³

En cierto modo, el acoso cibernético es peor que el abuso físico de un bravucón. Cuando una persona es víctima de intimidación en la escuela o en el patio de recreo, su vergüenza y malestar se limitan a

³ Centros para el Control y la Prevención de Enfermedades. (2014). Prevención de la intimidación. Extraído en línea en <https://www.cdc.gov/violenceprevention/youthviolence/bullyingresearch/fastfact.html>

las personas presentes. Cuando se retira del lugar físico, la intimidación cesa. De esta forma, la persona puede escapar de la situación.

En el acoso cibernético no existe esa posibilidad. Un bravucón puede seguir a la persona en forma virtual y seguir acosándola aun cuando no está junto a ella. Además, el malestar de la persona sigue presente para que todos lo vean. En este sentido, el acoso cibernético puede ser peor que la intimidación física porque no tiene salida.

Si eres víctima de acoso cibernético no debes avergonzarse. Tú eres la víctima, y no has hecho nada malo. Pero es necesario que tomes medidas para evitar que eso continúe:

- 1 No tomes represalias. Es comprensible querer defenderse y publicar cosas desagradables en línea sobre el bravucón. Sin embargo, eso no resolverá la situación y esta podría convertirse en algo peor.
- 2 Documenta la intimidación. Asegúrate de hacer capturas de pantalla de los mensajes y las publicaciones para que no puedan ser borradas. Registra la fecha y la hora de los mensajes, como también quién los envió.
- 3 Involucra a un adulto. Comparte las imágenes de los mensajes del bravucón con un padre, una maestra o con otro adulto. Dile cómo te hacen sentir estos mensajes, y pídele que te ayude a resolver la situación.

Recuerda que el acoso cibernético es más difícil de advertir para los padres, maestros o adultos, así que es esencial que informes a un adulto que estás siendo víctima de acoso en línea.

ACTIVIDAD

Luego de hablar sobre algunos de los problemas a los que los niños están expuestos en línea, use este sencillo juego para reforzar lo aprendido.

Preparación

Imprima suficientes copias de los dos emojis incluidos (página 14), para que cada niño/a tenga uno de cada uno. Considere imprimirlos en el anverso y reverso para ahorrar papel. También puede unirlos a varas de madera si desea. Si no tiene acceso a una impresora, los niños pueden usar sus manos, con el pulgar hacia arriba para expresar su acuerdo, o con el pulgar hacia abajo para mostrar su desacuerdo.

Cómo jugar

Lea la lista de situaciones a la clase e indique a los niños que usen los emojis para responder si esa actividad es «*acertada*» o si es algo que deben «*evitar*».

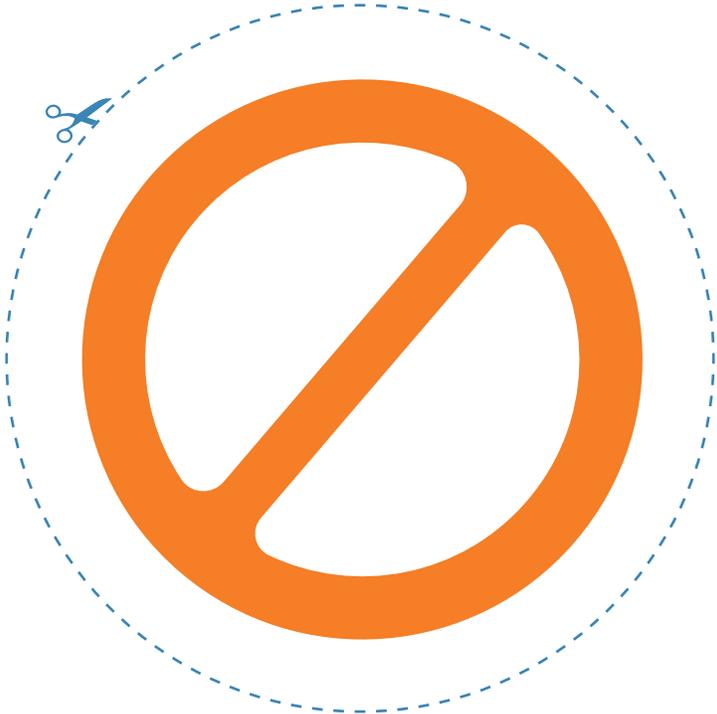


La mayoría responderá bien a las preguntas, y es probable que los que respondan mal se hayan equivocado al levantar el emoji. Si alguien responde mal a la pregunta, aproveche la oportunidad para reforzar el principio que la situación quiere enseñar.



Situaciones

- Usar el nombre de tu gato y tu año de nacimiento como contraseña.
- Decirles a tus amigos que dejen de burlarse de un/a compañero/a de clase en línea.
- Verificar que un enlace en un correo electrónico de tu abuela es seguro antes de hacer clic en él.
- Registrarte en una nueva plataforma de redes sociales sin hablar primero con tus padres.
- Aceptar la solicitud de amistad de alguien a quien no conoces, siempre y cuando la persona diga que conoce a tus padres.
- Investigar un poco antes de aceptar una solicitud de amistad, para asegurarte de que la persona sea quien dice ser.
- Tener una conversación privada en un salón de Zoom con uno de tus líderes juveniles o con un miembro del personal de Conquistadores.
- Eliminar de inmediato correos electrónicos, mensajes de texto o mensajes privados de personas a quienes no conoces si hay un enlace en el mensaje.
- Compartir memes que se burlan de personas de otras culturas u otros países
- Informar a un adulto si te están acosando en línea.
- Pensar en lo que quieres publicar en línea antes de pulsar Enviar, especialmente si estás enfadado/a o es tarde por la noche.
- Ajustar tus configuraciones de privacidad de redes sociales de manera tal que solo tus amigos puedan ver tus publicaciones y tu información.
- Hacer clic en el enlace que ofrece un 80 % de descuento en los AirPods Pro, que tu amigo/a compartió en su historia de Instagram.
- Compartir imágenes inapropiadas de ti o de otra persona.
- Evitar las estaciones públicas de carga USB.
- Usar una contraseña diferente para cada cuenta que tengas.
- Hablar mal de un/a compañero/a de clase en un chat privado porque este/a nunca lo verá.
- Publicar en línea una foto de tu casa.
- Bloquear y denunciar a cualquiera que te envíe fotos o comentarios inapropiados.
- Publicar en las redes sociales que esta tarde vas a estar en el centro comercial de tu localidad sin un adulto que te acompañe.
- Informar a un adulto si alguien en línea intenta hacer que te encuentres con él/ella en algún lugar.
- Suponer que todo lo que pones en línea es público.
- Compartir el enlace de tu clase Zoom en línea en el canal público Discord.
- No tomar represalias si te están acosando.
- Usar solo números en tu contraseña.



PREGUNTAS PARA EL DEBATES

Use las siguientes preguntas para iniciar un debate con sus alumnos sobre cómo usan la internet y las redes sociales y cómo creen que estarían más seguros en línea.

¿Cuáles son algunas de sus aplicaciones favoritas o sitios web favoritos para visitar? ¿Están en alguna aplicación de redes sociales? Si es así, ¿cuál/cuáles usan más a menudo?

Sin contar la escuela y/o la tarea, ¿cuánto tiempo por día creen que pasan en internet cada semana? ¿El tiempo aumentó o disminuyó durante la pandemia? ¿Qué tipo de cosas se pierden cuando pasan tiempo en línea?

¿Cuáles son algunas de las cosas positivas y negativas de las redes sociales? ¿Creen que las cosas positivas pesan más que las negativas? ¿Las cosas negativas pesan más que las positivas? ¿O pesan lo mismo?

¿Qué tipo de restricciones imponen sus padres en cuanto al uso de internet/redes sociales? ¿Por qué creen que tienen esas restricciones? ¿Deberían tener más restricciones de las que tienen actualmente?

¿Dónde obtienen noticias e información en internet? ¿Cómo pueden estar seguros de que los «hechos» que ven son exactos? ¿Por qué creen que algunos sitios o cuentas de redes sociales comparten información que no es exacta? ¿Qué pueden hacer cuando encuentran información incorrecta en línea?

¿A qué presiones de pares están expuestos los jóvenes en lo que se refiere a internet y a las redes sociales? ¿Estas presiones provienen principalmente de personas conocidas, personas desconocidas o de celebridades y/o influyentes?

¿Qué ejemplos de acoso cibernético han visto? ¿Fueron ustedes las víctimas del acoso, u otras personas? ¿Cómo reaccionaron a esos incidentes? ¿Cómo debieron haber reaccionado?

Es evidente que internet no existía en la época del ministerio de Jesús. Si hubiera existido, ¿cómo creen que Él habría usado estas herramientas en Su ministerio? ¿Cuáles son algunas maneras en que su iglesia podría usar internet o las redes sociales para transmitir el Evangelio? ¿Cómo pueden usar su presencia en línea para mostrar el amor de Dios?



Adventist Risk Management,® Inc. (ARM) está dedicado a la seguridad y al éxito de su ministerio. Ofrecemos recursos de gestión de riesgos para ayudarlo a proteger a las personas y los activos físicos que forman parte esencial de su ministerio. *Nuestro ministerio es **proteger** a su ministerio.* Conozca más en AdventistRisk.org/About-Us.
#ARMcares



INFORME SU RECLAMO DE INMEDIATO
1.888.951.4276 • CLAIMS@ADVENTISTRISK.ORG

MANTÉNGASE INFORMADO
ADVENTISTRISK.ORG/SOLUTIONS



Este material contiene información general basada en hechos, y bajo ninguna circunstancia debe considerarse asesoramiento legal referido a un asunto o tema en particular. Por favor, consulte a un abogado de su localidad si desea saber cómo se trata en su jurisdicción cualquier circunstancia específica que usted deba resolver.