



World Association
of Girl Guides
and Girl Scouts

Association mondiale
des Guides et des
Eclaireuses

Asociación
Mundial de las
Guías Scouts



**SURF
SMART**

**NAVEGACIÓN
INTELIGENTE**

“A las emisoras de radio les tomó 38 años para llegar a una audiencia de 50 millones, a la televisión 13 años, y al Internet sólo 4”

Este programa ha sido posible en parte gracias a una subvención de la Fundación Symantec, un fondo corporativo designado de la Fundación Silicon Valley Community.

Escrito por Andii Verhoeven y con la colaboración técnica de Marian Merritt.

Editado por Nefeli Themeli & Timothy Findlay.

Diseñado por Andriana Nassou.

2a edición

© WAGGGS, 2015

World Association of Girl Guides and Girl Scouts

World Bureau

12c Lyndhurst Road London NW35PQ, England

Teléfono: +44 (0)20 7794 1181

Facsímil: +44 (0)20 7431 3764

Email: waggs@waggs.org

Sitio web: www.waggs.org

Registered Charity No. 1159255 in England and Wales



Contenido

Introducción	4
Cómo utilizar este paquete y ganar una insignia	5
Cómo obtener tu insignia en tu país	5
Consejo para dirigentes	5
Actividades para ganar una insignia	5
Consejo para dirigentes	6
Conectarte...positivamente en línea	8
Protegerte...a ti mismo de los riesgos en línea	17
Respetar...tus derechos y tu reputación en línea	26
Ponerte en Primer Lugar	35
Directrices de seguridad en internet para adultos	38
Política de correos electrónicos	38
Política de redes sociales	38
Política de fotos y video	39
Seguridad general en línea	39
Proteger a los miembros del grupo	39
Recursos y enlaces	40
Seguridad en Internet	40
Oportunidades de Aprendizaje	40
Glosario	41

Introducción

¿Puedes imaginar la vida sin Internet?

En 2014, la población de internet en el mundo llegó por primera vez a 3 mil millones, equivalente a casi el 40 por ciento de las personas del planeta. A medida que se desarrolla la tecnología siempre estamos encontrando nuevas maneras de integrar el internet a nuestras vidas, y se prevé que para 2020, habrá 7 veces más aparatos conectados al internet como personas en el planeta.

La Asociación Mundial de las Guías Scouts (AMGS) reconoce la importancia del internet en nuestras vidas y también las amplias oportunidades que ofrece a sus miembros. Una Guía en Perú o Kenia ahora puede conectarse con una hermana en Canadá, Corea del Sur o India, favoreciendo un mayor acercamiento en el Movimiento y permitiendo que las niñas y las jóvenes se conecten entre sí para compartir información y propugnar en temas que son importantes para ellas en sus comunidades, en sus países y en el mundo.



Con el uso generalizado de esta tecnología, es más importante que nunca garantizar que nuestros miembros puedan seguir utilizando el internet con seguridad, conectándose positivamente con otros en línea y respetando sus propios derechos y reputación en el mundo digital. Al igual que con cualquier riesgo, creemos que es importante trabajar con las niñas y las jóvenes para ayudarlas a construir su propio conocimiento y comprensión; ofrecerles oportunidades a través de las cuales puedan equiparse a sí mismas con las habilidades que necesitarán para disfrutar el uso de la tecnología del internet con seguridad y a su máximo potencial y desarrollar habilidades, conciencia y confianza en el manejo de los riesgos asociados con la misma.

Al asociarse con Symantec, una de las mayores empresas de seguridad en internet en el mundo, para producir este programa, la AMGS espera compartir la experiencia de la empresa en la seguridad en línea con sus miembros. Con el apoyo profesional y el asesoramiento de los profesionales en seguridad cibernética de Symantec y las actividades de los expertos en educación no formal de la AMGS, creemos que el programa Surf Smart ofrece un recurso único que garantizará una generación de niñas y mujeres jóvenes equipadas con las habilidades necesarias para protegerse a sí mismas y a otros en línea.

¡Naveguen felices!

Nicola Grinstead

Cómo utilizar este paquete y ganar una insignia

Sólo poco más del 40 por ciento de la población mundial tiene acceso a internet. Si estás conectado, probablemente el internet juega una parte importante en tu vida. Lo usas para responder preguntas, compartir con tus amigos y disfrutar tu tiempo libre. Surf Smart te lleva en una aventura digital para explorar cómo puedes sacar el mayor provecho de tu tiempo en línea y conectarte con comunidades locales y globales, y cómo mantenerte seguro y tomar buenas decisiones cuando estás conectado.



Surf Smart contiene un montón de actividades divertidas que te ayudarán a desarrollar nuevas habilidades y conciencia digital. Cuenta con tres temas:

Conectar positivamente en línea (p. 8)

Proteger a ti mismo de los riesgos en línea (p. 17)

Respect tus derechos y reputación en línea (p. 26)

Presta atención a otros datos interesantes que te pueden ayudar a completar las actividades, y los mejores consejos para sacar el mayor provecho de tu tiempo en línea. Mientras trabajas en el paquete es posible que encuentres palabras que son nuevas para ti; éstas se explican en el glosario en la página 41.

Cómo obtener tu insignia en tu país

Cuando completes el programa, recibirás la insignia de “Surf Smart”. Para obtenerla contacta a tu organización a la siguiente dirección para que te sea enviada.

Actividades para ganar una insignia

Elige dos actividades de cada tema (Conectar – Proteger – Respetar) además de la actividad “Ponte en Primer Lugar” en la página 35 para ganar tu insignia





Tiempo



Materiales



Edad



Cuadro de Información

Consejo para dirigentes

- La seguridad en internet es un problema creciente a medida que los jóvenes encuentran más maneras de hacer que el internet sea parte de su vida cotidiana. Este paquete tiene como objetivo crear conciencia sobre la seguridad en internet en el mayor número posible de Guías y Guías Scouts. Tú puedes ayudar adaptando las actividades y los requisitos de la insignia para que Surf Smart sea accesible para tus miembros. – ¡tú los conoces mejor!
- Las actividades de este paquete han sido desarrolladas para miembros de la AMGS de todas las edades y de ambos sexos, y cuentan con aportaciones de una serie de países. Algunas actividades han sido marcadas como más adecuadas para miembros mayores o más jóvenes, pero por favor usa tu propio criterio en el momento de seleccionar las actividades para tu grupo. Si bien es importante que nuestros miembros sepan cómo mantenerse seguros en cualquier situación en línea, Surf Smart alienta, pero no presiona a los miembros para entrar en línea, y puede ser utilizado en entornos sin acceso a internet.
- Los tiempos sugeridos para cada actividad son una guía para ayudarte con tu planificación. Dependerá del tamaño de tu grupo y qué tanto estás adaptando las actividades.
- Examina la información de este paquete antes de comenzar las actividades. A lo largo del paquete hay 'cuadros de información' que proporcionan la información que tienes que compartir con los miembros jóvenes antes, durante o después de cada actividad. Los enlaces en línea que hemos elegido se consideran apropiados para una audiencia joven, pero te aconsejamos que los revises antes para asegurarte de sentirte cómodo de compartirlos con el grupo
- Recomendamos que las actividades que requieren tiempo en línea estén restringidas para miembros de 13 años y mayores. Esto se debe a que algunos servicios en línea comúnmente utilizados, como Facebook y YouTube, no están destinados a niños menores de 13 años. Sin embargo, ésta es solo una guía y tal vez tú consideres que muchas de estas actividades son apropiadas para los miembros más jóvenes. Debido a que ahora los niños aprenden a utilizar el internet tan pronto como empiezan la escuela, o antes, creemos que es importante que

nuestros miembros comiencen a aprender sobre la seguridad en internet lo antes posible.

- Es tu responsabilidad asegurarte de que todas las medidas de protección necesarias estén en marcha y se hayan obtenido los consentimientos en el momento de utilizar este recurso. Por favor utiliza las directrices de seguridad en internet para adultos de la página 36 para apoyar esto.
- Te invitamos a agregar cualquier contenido relevante que descubras en tu propia investigación. Encontrarás videos, música, fotos, juegos y un montón de información en YouTube y en los sitios web que aparecen en la parte posterior del paquete.

¡Comparte!

Por último, ¡sería increíble compartir tu experiencia Surf Smart, las fotos que tomaste y los videos que creaste, con las Guías y Guías Scouts de todo el mundo!

¡Hay muchas maneras de conectarte con la AMGS!



Visita www.waggs.org



Twitter (@waggs_world)



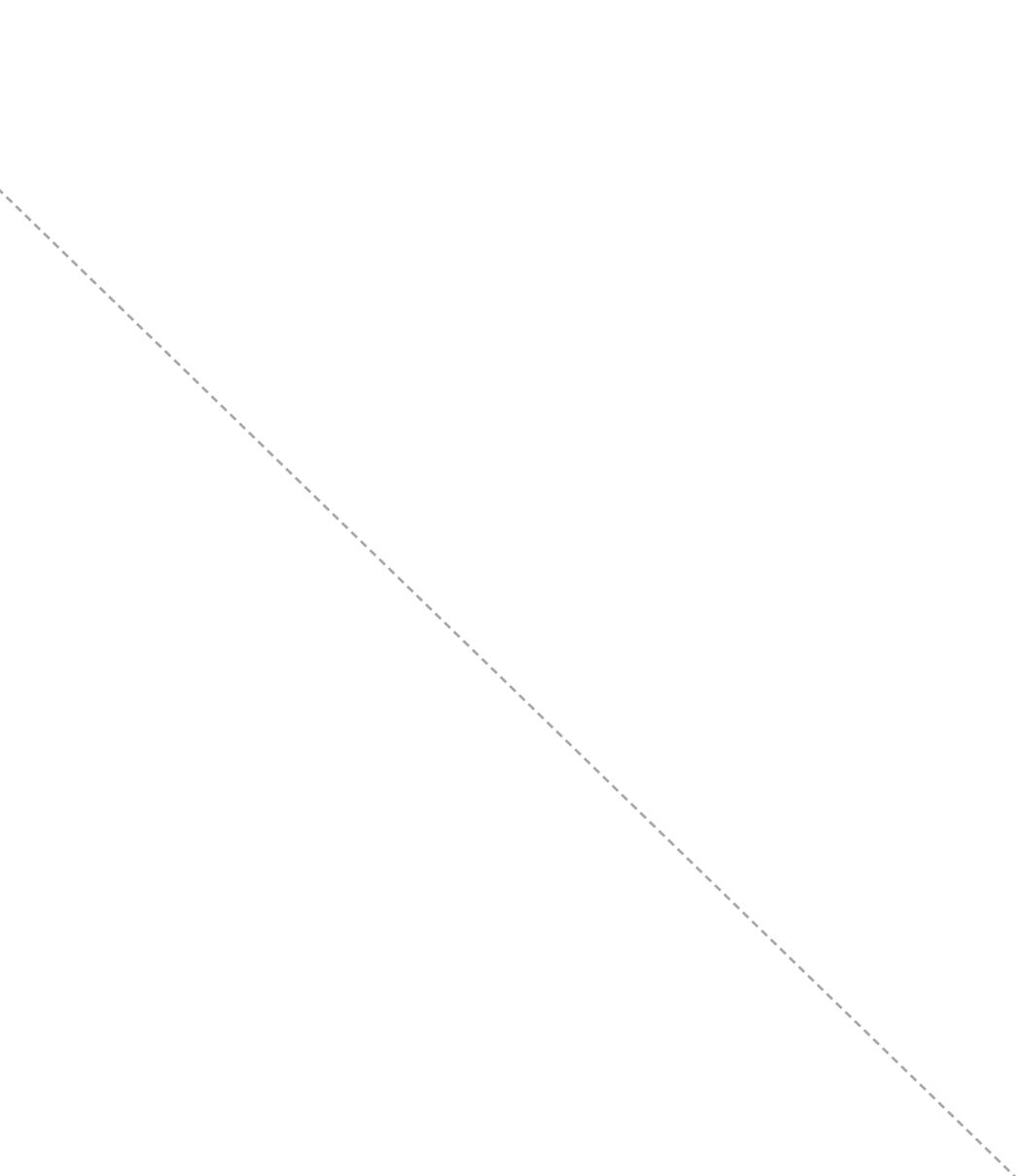
Facebook
(www.facebook.com/waggs)



Dinos qué piensas del paquete de actividades, completando una encuesta en línea:
www.waggs.org/es/internetsafety



Envía tu historia Surf Smart por correo electrónico a
youthlearning@waggs.org



EMPECEMOS

Conectar...positivamente en línea

¡Completa dos actividades para ganar tu insignia!

¡CONSEJO!

Cuida a tus amigos en línea;
si piensas que están en riesgo,
¡Toma medidas!



1 Qué significa para mí

El internet se ha convertido muy rápidamente en una parte importante de nuestra vida. Elabora una lista de las maneras en que piensas que el internet afecta tu vida, tanto positiva y negativamente. Pregunta a personas que conozcas de otra generación, por ejemplo, padres y abuelos, cómo utilizan el internet en su vida cotidiana. ¿Qué diferencia hay entre sus respuestas y las tuyas? Prepara una exhibición con las respuestas mediante el uso de carteles, folletos, publicaciones de blogs o videos.



15 mins



Suficiente papel, lápiz, lápices de colores para todos los participantes

TODAS LAS EDADES

Llévalo más lejos – Elige a alguien de una generación anterior que consideres que ha cambiado el mundo, como Emmeline Pankhurst, Mahatma Ghandi, Rosa Parks o Nelson Mandela. ¿Qué crees que habría hecho diferente si hubiera tenido una cuenta en una red social?



10 min



Redes sociales

Las redes sociales son una parte importante de la vida en línea. Hacen que sea muy fácil mantenerse en contacto con amigos y explorar un montón de nuevos contenidos como videos, fotos y chats, todo en el mismo servicio web.

- Comprueba tu configuración de privacidad y pide a un amigo o familiar que vea tu perfil para asegurarse de que no estás publicando información que sería preferible no mostrar. Cuando vemos nuestra red social todos los días, es muy fácil pasar por alto cosas simples que sería mejor guardar para nosotros mismos.
- Lee sobre la reputación digital y la creación de contenidos para internet, ya que son temas realmente importantes cuando se están utilizando las redes sociales.
- Si eres menor de 13 años, se supone que no debes tener una cuenta de Facebook.
- Si alguien te pide que seas su 'amigo' en línea, no hagas clic en "sí" de manera automática. ¿Realmente conoces a esta persona? En caso negativo, piensa si quieres que tenga acceso a tu perfil y publicaciones.



2 ¿Corta o larga?

Proporciona a cada participante tres objetos para incluirlos en una historia. La mitad del grupo debe inventar una historia de cualquier tamaño. La otra mitad solo puede usar 140 caracteres para escribir su historia. Compartan las historias. ¿A qué grupo le resultó más fácil contar una buena historia?



10 mins



papel, lápiz, 3 objetos



Llévalo más lejos – Las publicaciones cortas en las redes sociales pueden hacer que sea difícil transmitir tu mensaje. Usando tu cuenta de grupo, trata de compartir tu historia usando diferentes medios sociales como Facebook, twitter, Google+, tumblr, VK, etc. ¿Qué tipo de mensajes crees que funcionan bien en las redes sociales? ¿Hay otros mensajes que sería mejor compartir de diferentes maneras?



10min



computadora/tablet/teléfono inteligente con acceso a internet



3 ¿Cuál es el mensaje?

Proporciona a cada participante un pedazo de papel y siéntense en un círculo. La primera persona susurra una palabra a su vecino, quien a su vez hace un dibujo de lo que escuchó y lo pasa a la tercera persona, quien susurra lo que ve a la siguiente persona y así sucesivamente, alternando el mensaje entre palabras e imágenes. ¿Es el mismo mensaje cuando regresa al principio? Comienza con objetos o frases simples y luego hazlo más complejo. Pide a tu dirigente que seleccione secretamente a alguien en el círculo para cambiar una palabra del mensaje. ¿Podrías decir en dónde cambió?

Discutan: ¿Cómo pueden cambiar los mensajes en línea? Una vez que has publicado información en línea, ¿cuánto control tienes sobre ella?



10 mins



papel, lápiz

TODAS LAS EDADES

Casi el **40%**

de la población mundial utiliza el internet

4 Conéctate

El internet no es la única manera de conectar a las personas. Como Guía & Guía Scout, tú formas parte de un Movimiento mundial que reúne a jóvenes de 146 países. Investiga diferentes maneras de ponerte en contacto con un grupo Guía & Guía Scout en otro país, o con uno de los Centros Mundiales de la AMGS. Muestra tus planes a tu dirigente y luego pruébenlos juntos. Los métodos incluyen correo electrónico, teléfono en línea, video llamada, y enviar una carta a un grupo que hayas encontrado en línea.

Es muy emocionante estar en contacto con personas de otras culturas, pero es importante entender y respetar las diferencias en sus vidas. Esto es tan cierto cuando te conectas a través de internet como lo sería si se encontraran en persona.

Investiga su sociedad y su cultura y trata de hacerles preguntas no prejuiciosas para aprender más sobre sus vidas. Si te conectas en tiempo real, no olvides tomar en cuenta la diferencia de horario.



20 mins



computadora/tablet/teléfono
inteligente con acceso a internet,
papel, lápiz



Llévalo más lejos – Crea una cuenta de SKYPE para tu grupo y ponte en contacto con diferentes miembros de la AMGS por esta vía.

Por favor visita:

www.waggs.org/es/internetsafety para obtener más información sobre cómo conectarte



20 min



computadora/tablet/teléfono
inteligente con acceso a internet



5 Hazlo local

No se trata solo de conexiones mundiales, el internet puede ser una gran herramienta para ponerte en contacto con tu comunidad local y compartir oportunidades. Pero ¿qué pasa si no puedes encontrar los datos que necesitas? Investiga la presencia de tu comunidad en línea – ¿podría ser mejor? Averigua las oportunidades disponibles para los jóvenes en tu comunidad, e investiga cómo podrían utilizar un portal en internet, como un sitio web o una página de Facebook, para correr la voz y mejorar el acceso a la información y a las oportunidades de tu comunidad.



esta actividad requiere prepararse
e implementarse en más de una reunión



computadora/tablet/teléfono
inteligente con acceso a internet



Llévalo más lejos – ¿Cómo podrías utilizar el internet para poner en marcha un proyecto en la comunidad? Algunos grupos comunitarios muy exitosos utilizan el internet para conectar a las personas que buscan un terreno para cultivar sus propios alimentos, con propietarios de terrenos no utilizados en la comunidad. Otros lo utilizan para anunciar artículos que desean reciclar o para promover que las personas intercambien habilidades, por ejemplo, alguien que puede enseñar español y busca a alguien que puede enseñar habilidades básicas de computación. ¿Qué tal un grupo que reúna y comparta oportunidades de voluntariado para los jóvenes? Haz un sondeo en tu comunidad e identifica una necesidad que consideres que puede cubrirse a través del uso del internet.

Conoce más sobre los proyectos de acción comunitaria de la AMGS:

www.waggs.org/es/grab/25247/1/bethechange-sp-web.pdf



¡CONSEJO!

¿No te gusta lo que alguien está diciendo? Pulsa bloquear.

6 Aventura en línea

Una de las cosas increíbles del internet es que pone justo en tu pantalla, oportunidades que ni siquiera sabías que existían. ¿Cuál sería tu máxima aventura? ¿Tal vez un viaje a un país del que nunca habías oído hablar, o un reto poderoso que acelere tu pulso? Imagina tu aventura perfecta, luego utiliza el internet para organizar un álbum virtual de tu viaje con la información y los medios que puedes encontrar en línea. Comparte tu aventura con tu grupo y colocala en un lugar donde puedas verla en casa para inspirarte.



15 mins



computadora/tablet/teléfono inteligente con acceso a internet y una impresora



Llévalo más lejos – ¿Qué tal si tu sueño se hiciera realidad y realmente pudieras hacer la reserva para tu aventura? Investiga cómo podrías utilizar el internet para planificar el itinerario perfecto, Obtén información privilegiada y localiza las mejores ofertas. Sin embargo, no todas las ofertas son tan buenas como parecen, así que aprende a detectar los fraudes vacacionales. Visita algunos de los sitios web seguros que aparecen en la parte posterior del paquete, donde encontrarás consejos sobre el uso de internet en la planificación de viajes.



20 min



computer/tablet/smartphone with internet access



7 ¡Bloquéalo!

Organiza un trayecto con obstáculos en el lugar de reunión. Venda los ojos a dos miembros del grupo y pídeles que caminen de un extremo a otro del trayecto. Cada uno tiene un 'guía' que camina con ellos, pero el guía sólo puede ayudarlos con su voz. ¿Qué tan fácil es recorrer el trayecto sin tocar los obstáculos?

Discutan: Este juego es un poco como conectarse en línea; la persona con los ojos vendados es como alguien que utiliza el internet y no siempre puede ver los riesgos de seguridad que le rodean. El guía representa el software de seguridad que puede ayudar al usuario a navegar en la web de manera segura. Sin embargo, el software de seguridad no puede hacer todo solo. La persona con los ojos vendados tiene que cooperar y ser cuidadosa, usar sus otros sentidos y no apresurarse. Cuando se utiliza el internet, los usuarios tienen que ser lo más inteligentes y cuidadosos que puedan. Eso, combinado con un buen software de seguridad, los ayudará a mantenerse seguros en línea.

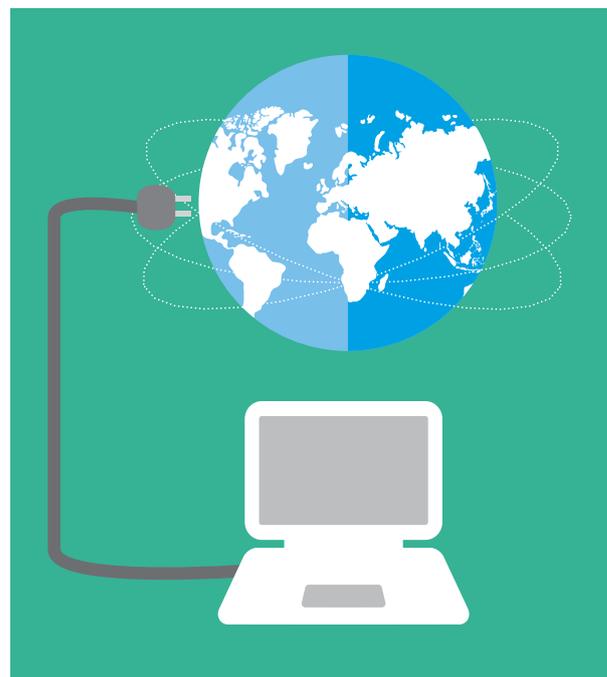


15 mins



objetos para obstáculos, un pañuelo o venda para cada participante

TODAS LAS EDADES



Una simple consulta en Google utiliza **1,000** computadoras en **0.2 seconds** para obtener una respuesta

8 Lo mejor de la web

Hay muchos sitios web increíbles, pero no puedes probarlos todos. En cambio, ¿Puedes compartir tus conocimientos con tus amigos! En grupos, hablen sobre sus sitios favoritos, lo que hacen y por qué les gustan. Hagan un mapa visual de los mejores sitios web que recomienda su grupo, y ordénenlos de acuerdo a su uso, por ejemplo, redes sociales, escuchar música, aprender sobre actividades al aire libre o juegos. ¿Cómo crees que podría ayudar esta lista a alguien que está buscando nuevos sitios o que entra en línea por primera vez?



20 mins



computadora/tablet/teléfono inteligente con acceso a internet, papel, lápiz, lápices de colores para todos los participantes

TODAS LAS EDADES

Llévalo más lejos – ¿Hay algo que tú sabes hacer en línea, que no sabe hacer alguien de una generación anterior? Habla con un adulto de confianza y averigua qué es lo que más le gustaría saber hacer en línea, luego enséñale cómo hacerlo. También puedes utilizar la lista de sitios web interesantes que elaboraste en la actividad anterior, como referencia y para ejemplos.



20 min



computadora/tablet/teléfono inteligente con acceso a internet

+13



Búsqueda segura

El internet es la biblioteca más grande que jamás encontrarás, y todos pueden contribuir a ella. Sin embargo, eso no significa que todo lo que encontrarás en línea es confiable. El contenido no siempre está escrito por expertos, y las personas pueden tener una gran cantidad de opiniones diferentes que afectan su manera de escribir sobre algo.

Entonces, ¿cómo puedes estar seguro de que tus búsquedas te proporcionen información confiable?

- Usa más de una palabra para describir lo que estás buscando. Por ejemplo, si quieres saber más sobre la cultura musical de Brasil, busca "cultura musical de Brasil" y obtendrás información más específica que si escribes sólo "Brasil".
- Detente y piensa en las palabras que estás usando antes de pulsar "buscar". ¿Alguna de ellas tiene otro significado que podría traer resultados no deseados?
- Verifica tu información. No puedes confiar en todo lo que encuentras en línea, así que sé un buscador inteligente y consulta al menos tres sitios para verificar la información, y no olvides buscar en libros o hablar con personas que conoces.
- Revisa tus filtros de búsqueda, en particular si estás buscando imágenes, para evitar material inapropiado. Verifica tu configuración de búsqueda y selecciona los ajustes de seguridad más altos
- ¿Quieres volver a un sitio que ya visitaste? Agrega a tu lista de sitios favoritos o revisa tus listas de historial para asegurarte de volver a visitar la misma página.
- ¡Comprueba tu ortografía! Un pequeño error de escritura en tu búsqueda puede traer resultados que no deseas

El software de seguridad te puede proteger de los sitios web falsos. Descarga las herramientas del navegador o utiliza las de tu software de seguridad para identificar sitios impostores y mantener búsquedas seguras. Algunas también pueden mostrar las valoraciones del sitio.

¡CONSEJO!

¿Alguien está actuando inapropiadamente en un programa de mensajería instantánea, sala de chat o juego en línea? Utiliza el botón de Impresión de Pantalla para tomar una imagen de la pantalla de los mensajes, luego abre un programa de dibujo, pega la imagen de la pantalla y guárdala como evidencia.



9 Búsqueda del tesoro de texto

¿Cómo puedes utilizar la tecnología móvil para actualizar una actividad familiar? Trata de organizar una búsqueda del tesoro de texto o correo electrónico para tu grupo. Explora tu área local y piensa en pistas que tu grupo podría seguir para encontrar lugares específicos, así como una pregunta sobre cada lugar, que sólo podrán resolver una vez que se encuentren en el lugar. Manda al grupo con un teléfono móvil y envíales un mensaje de texto con la primera pista y pregunta. Cuando te envíen la respuesta, envíales un mensaje de texto con la pista y la pregunta para el siguiente lugar. ¿Cómo cambia la experiencia el uso de un teléfono móvil?



30 mins



computadora/tablet/teléfono
inteligente con acceso a internet por
grupos internet access per group



Llévalo más lejos – Prueba otras formas de utilizar la tecnología móvil en las actividades. Considera incorporar apps de un teléfono inteligente y establece un reto en el que los miembros jóvenes tengan que utilizar al menos 5 apps diferentes en su teléfono, como: Google maps, QR codes (un tipo de código de barras que puede leer tu teléfono), grabadora de voz, calculadora, brújula, cámara, etc.



30 min



computadora/tablet/teléfono
inteligente con acceso a internet por
grupo



Volverse móvil

Navegar en la web ya no solo tiene que ver con las computadoras. Con los teléfonos móviles, tablets y consolas de juegos portátiles, ahora puedes estar conectado casi en cualquier lugar. Es tan importante hacer un uso inteligente de estos dispositivos, como lo es el uso de tu computadora personal. Algunas directrices básicas son:

- Cualquier cosa enviada en un mensaje instantáneo o SMS se puede reenviar o compartir fácilmente, así que piénsalo dos veces antes de enviar algo que no quieres que vea alguien más.
- La mayoría de los dispositivos móviles pueden estar protegidos con una contraseña. Establece una contraseña en tu teléfono – ¡Impide el acceso a tu información en caso de pérdida o robo, e impide que tus amigos lo utilicen sin tu permiso!
- Todavía no hay muchos virus de teléfonos móviles, pero sí los hay. Ten cuidado al hacer clic en un enlace desconocido o responder un texto inesperado. Verifica que el software de seguridad de la marca de tu teléfono móvil esté a la altura.
- Nunca proporciones el número de tu teléfono móvil a alguien que conociste en línea pero que no conoces en persona.
- Mantente alerta a lo que estás gastando y conoce tu límite.
- Ten cuidado con el tiempo que pasas en tu teléfono, especialmente en la noche antes de ir a dormir. Hay estudios que advierten a los usuarios de teléfonos móviles y tablets sobre el uso de las pantallas intensamente iluminadas, ya que alteran los ritmos naturales del organismo y se traducen en mala calidad del sueño.

TIP!

¿Utilizas tu teléfono móvil cuando estás fuera de casa? Ten en cuenta que si estás en una llamada, no necesariamente estás prestando mucha atención a tu entorno, así que trata de ser breve, sobre todo si ya es tarde.

DISCUTAN:

¿Qué haces para que tu blog sea totalmente privado?

10 ¿Escuela del futuro?

¿Has pensado que la tecnología ha afectado la manera en que aprendemos? Sugata Mitra, ganador del premio TED en 2013, introduce un tipo diferente de escuela: una escuela en la nube. Ve su inspiradora charla TED www.ted.com/talks/sugata_mitra_build_a_school_in_the_cloud?language=es donde presenta su proyecto. Discute con el resto del grupo lo que piensas al respecto. ¿Te interesaría una escuela como esa? ¿En qué es diferente a tu escuela? ¿Estás de acuerdo con este punto de vista?



40 mins



computadora/tablet/teléfono
inteligente con acceso a internet



Llévalo más lejos – Conoce más sobre el proyecto de Sugata Mitra, basado en Entornos de Aprendizaje Auto-organizados (SOLE) www.ted.com/talks/sugata_mitra_build_a_school_in_the_cloud?language=es. Comparte tu opinión utilizando la cuenta de redes sociales de tu grupo, invita a tus amigos a compartir sus opiniones.



20 min



computer/tablet/smartphone
with internet access



Blogging

Los blogs son una publicación en línea donde las personas comparten sus opiniones y sentimientos, y capturan momentos de sus vidas en texto, imágenes y videos. Puedes hacer que tu blog sea privado y compartirlo con personas que conoces o hacerlo público. Los blogs son una gran manera de practicar tus habilidades de redacción y ser creativo, y también puedes utilizarlos para conectarte con otras personas que comparten tus intereses. Los blogs funcionan mejor si se apegan a un tema o interés particular. En lugar de describir lo que desayunaste, enfócate en algo que amas - ¡entre más específico, mejor! Sin importar lo que publiques, verifica la seguridad de tu blog

Consejos para publicar de manera segura

- Verifica tu configuración de seguridad antes de hacer una publicación.
- Si todos los que conoces pueden tener acceso a tu blog, no publiques nada que no quisieras que vieran todos tus conocidos.
- Retira toda la información personal de tu blog o perfil que podría ser utilizada para identificarte, como nombre completo, edad, ubicación, número de teléfono, o nombre de tu escuela.
- Aprende a manejar los comentarios o a bloquearlos por completo. Debes estar preparado para monitorear los comentarios inapropiados y retirarlos de tu blog.
- Recuerda que una vez que se publica algo en línea, no se puede retractar. Aunque elimines una publicación, su contenido podría haber sido copiado.
- Si algo en tu blog te hace sentir incómodo, como por ejemplo, que otros hagan comentarios que no te gustan, habla con un adulto en quien confíes.
- No inicies un blog solo por el gusto de hacerlo. Espera hasta tener una idea clara de lo que quieres escribir.

Muestra tu blog a un adulto de confianza y pídele que vigile lo que se publica allí.

En **1 segundo** hay:

8,480 Tweets enviados,
1,701 fotos de instagram compartidas,
1,720 publicaciones tublr,
1, 651 llamadas de Skype,
95,156 videos vistos en YouTube,
2,367, 473 correos electrónicos enviados



11 Publica acerca de esto

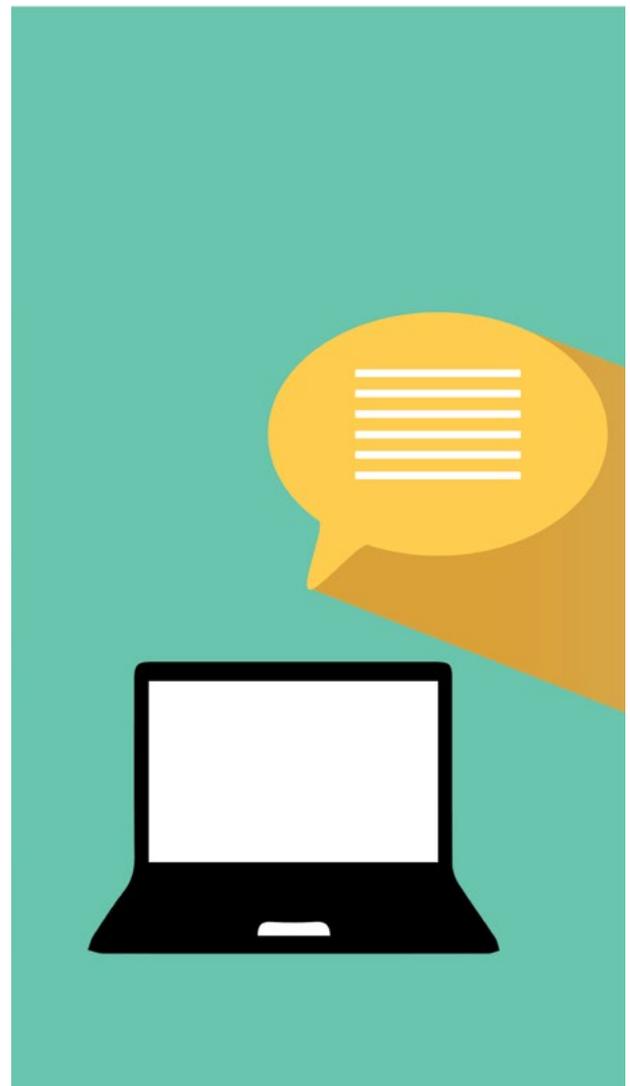
¿Alguna vez has pensado en iniciar un blog? Los blogs son una gran manera de practicar tus habilidades creativas, como la redacción y la fotografía, pero es importante planificar de antemano lo que vas a publicar y tener una idea clara de la información que estás dispuesto a que aparezca en tu blog, y lo que quieres guardar solo para ti. Los blogs más exitosos se centran en temas que interesan a las personas. ¿Qué sabes acerca de, o quieres aprender más acerca de? Haz una lista de los temas sobre los que crees que te gustaría escribir y compartir con tu grupo. ¿Qué lecturas les parecen más interesantes a tus amigos? Crea un blog privado para compartir con tus amigos y familiares y mantenlo actualizado por un tiempo.



esta actividad requiere prepararse e implementarse en más de una reunión



computadora/tablet/teléfono inteligente con acceso a internet



¡CONSEJO!

Recuerda cerrar la sesión cuando hayas terminado con una página web.

12 Historia en fotografías

¿Te gusta tomar fotos? ¿Por qué no las usas para contar tu propia historia! Decide qué mensaje quieres compartir, planifícalo como una serie de imágenes, y toma fotos que, cuando las exhibas en un orden determinado, digan lo que quieres decir.



20 mins



cámara/tablet/teléfono inteligente e impresora

Llévalo más lejos – Sube tu historia a internet utilizando un servicio que te de control de la privacidad, como Flickr, Google+ Fotos, Instagram o un grupo de Facebook, para que puedas controlar a quiénes invitas a ver tu historia, luego compártela con amigos y familiares. Aprende cómo proteger tus fotos con marcas de agua y cómo impedir que otros copien tus imágenes, luego inténtalo tú mismo.

Recuerda que puedes compartir tus fotos con Guías y Scouts de todo el mundo en www.waggs.org/es/internetsafety !



10 min



computadora/tablet/teléfono



Creación para Internet

Cuando subes tu contenido al internet, estás celebrando un acuerdo con el servicio web que estás utilizando. Ya sea que se trate de Facebook o YouTube, un sitio de blogging como Tumblr o un sitio de fotos como Flickr, al subir tu contenido estás aceptando los “Términos de Servicio” o “Términos de Uso” del sitio – las reglas de un proveedor de servicios en línea que los usuarios deben obedecer.

Cuando creas un contenido original, automáticamente tienes los derechos de propiedad del contenido. Un contenido original es cualquier cosa que fue creada 100 por ciento por ti – una grabación donde cantas una canción que tú escribiste, por ejemplo, no una canción escrita por otra persona. Cuando utilizas la mayoría de los servicios en línea, tú conservas esos derechos de propiedad del contenido. Sin embargo, los servicios en línea pueden utilizar tu contenido de muchas maneras, sin quitarte esos derechos de propiedad – puedes encontrarlas en los Términos del Servicio o Términos de Uso.

Si consultas los Términos de Uso de un servicio que utilizas, probablemente encontrarás una frase que se parece un poco a esto:

“Al enviar un contenido a nuestro Servicio, usted nos concede una licencia perpetua a nivel mundial, no exclusiva, libre de regalías para usar, copiar, adaptar, modificar, publicar, exhibir y distribuir su contenido en cualquier medio”

Eso significa que el servicio puede hacer lo que quiera con tu contenido, aunque siga siendo de tu propiedad. Lo pueden compartir con otros en todo el mundo durante el tiempo que lo deseen, cambiarlo en cualquier forma, publicarlo en cualquier forma, y proporcionarlo o venderlo a otras compañías para que hagan lo mismo. Estos términos no sólo aplican para videos y fotos, también pueden aplicar para posts y tuits en los sitios de redes sociales. La única manera de estar seguro de que estás contento con el uso que da el servicio web a tu contenido, es comprobando sus Términos de Uso.

Proteger...a ti mismo de los riesgos en línea

¡Completa dos actividades para ganar tu insignia!

¡CONSEJO!

Las restricciones de edad en línea están allí para impedir que veas algo que realmente no quieres ver. Si una página dice "18+", cierra la sesión y díselo a tus padres/cuidadores.



1 Muéstralo

En un grupo pequeño, decidan tres consejos básicos que consideren importantes para mantenerse seguros en línea. Hagan un baile, canción o espectáculo que comunique estos consejos, y preséntenlo a su grupo.



15 mins

TODAS LAS EDADES

Piensen en cómo podrían hacer que sus consejos básicos sean fáciles de entender para los miembros más jóvenes, luego presenten su obra a un grupo de menor edad. Después, hablen con ellos sobre el mensaje de su obra.



15 mins



Llévalo más lejos – Graben su actuación y súbanla al canal de YouTube de la AMGS. Recuerden verificar que todos los que participan estén contentos de aparecer en línea



15 min



¡CONSEJO!

Verifica las configuraciones de privacidad de los sitios donde publicas información.

DISCUTIR:

¿Qué debes hacer si alguien en un chat te pide que le envíes tu foto?

2 Una buena contraseña

Una buena contraseña utiliza una mezcla de letras, números y símbolos. Debe ser difícil de descubrir para otros, pero fácil de recordar para ti. En un grupo pequeño, tomen turnos para elegir un objeto inolvidable o una frase o refrán favorito, como una línea de tu libro o película favorita. Luego, cada persona piensa en cómo convertir esta frase en una contraseña difícil de descubrir pero fácil de recordar con al menos ocho caracteres, utilizando una mezcla de letras, números y símbolos. Para ayudar, dibuja una cuadrícula con dos líneas y tantas columnas como haya letras diferentes en tu contraseña. Si usas una frase, utiliza la primera letra de cada palabra. Escribe las letras en la línea superior y el símbolo o número correspondiente en la línea inferior.

Por ejemplo, la palabra "mariposa" que es fácil de adivinar, se convierte en "M@r1p0\$a", una contraseña mucho mejor.

M	A	R	I	P	O	S	A
M	@	r	1	p	0	\$	a

Escribe algunas contraseñas utilizando este código, luego dáselas a un amigo para ver si puede descifrarlas.

Discutir: ¿Puedes pensar en otras maneras de hacer una contraseña complicada que sea fácil de recordar?



10 mins



Suficiente papel y lápices para todos los participantes

Llévalo más lejos – Separa los grupos en equipos pequeños, para que cada equipo tenga un teléfono inteligente o una tablet. Pide a los grupos que busquen en línea las apps que se utilizan para la seguridad de contraseñas y protección de información. Permite que los equipos investiguen un momento y luego presenten sus sugerencias.



10 min



computadora/tablet/teléfono inteligente con acceso a internet



DISCUTIR:

¿Cuáles son tres maneras de hacer una mejor contraseña?



Buenas contraseñas

La clave para una buena contraseña es encontrar un equilibrio entre algo que puedes recordar y algo que nadie más puede descubrir.

Para estar seguro de tener una buena contraseña:

SÍ...

- Mantén tu contraseña al menos con ocho caracteres.
- Utiliza una mezcla de letras mayúsculas y minúsculas, números y símbolos.
- Cierra la sesión cuando hayas terminado con un servicio en línea.

NO...

- Uses solo palabras que puedes encontrar en un diccionario.
- Incluyas información personal, como tu nombre o cumpleaños.
- Uses algo obvio, como "12345678", "tequiero" o "contraseña".
- Uses la misma contraseña para todas las cuentas. Mantén contraseñas únicas para las cuentas realmente importantes, como tu correo electrónico o red social.
- Ingreses tu contraseña en formularios en línea o la envíes en correos electrónicos. Si recibes un correo electrónico de un sitio web que utilizas y te piden tu contraseña, probablemente es un intento de phishing y no proviene del sitio web
- Compartas tus contraseñas con amigos. No quiere decir que no confíes en ellos, simplemente es una buena práctica.
- Mantengas tus contraseñas en la pantalla. Si necesitas anotarlas, mantenlas en un lugar seguro fuera de la vista, puedes dárselas a tus padres. No las conserves almacenadas en tu computadora.

¡CONSEJO!

Conserva tu contraseña solo para ti y cámbiala con frecuencia.

Nunca hagas clic en una ventana emergente, incluso si dice “cerrar” o “cancelar”. Siempre usa la cruz roja para eliminarla.



DISCUTIR:

¿Quién debe tener una copia de tus contraseñas?

3 Manténla privada

Muchos lugares en línea, como las redes sociales, sitios de almacenamiento en la nube o juegos en línea, requieren la creación de una cuenta y perfil personal. ¿Sabes cuántas cuentas tienes? Al hacer uso del internet durante la próxima semana, enumera todos los lugares en línea donde tienes una cuenta. Da “luz verde” a tus cuentas, verificando que hayas elegido configuraciones de privacidad y hayas creado una contraseña segura para cada cuenta de tu lista.



10 mins



computadora/tablet/teléfono inteligente con acceso a internet, papel, lápices de colores



4 Vence al virus

¿Qué es un virus informático? ¿Por qué la gente crea los virus? ¿Cómo se propagan? ¿Cómo puedes proteger tu computadora contra ellos? Invita a un maestro TIC o experto en computación para que visite a tu grupo, responda estas preguntas y explique cómo funciona el software de seguridad en internet para mantenernos seguros. También puedes investigar en línea - mx.norton.com/virus-first-written/article es un buen lugar para empezar - presenta a tu grupo lo que has aprendido.



esta actividad requiere prepararse e implementarse en más de una reunión



computadora/tablet/teléfono inteligente con acceso a internet

TODAS LAS EDADES

¡CONSEJO!

Si quieres enviar un correo electrónico, recuerda que no puedes controlar con quién se compartirá una vez que pulsas "enviar". Protege las direcciones de correo electrónico de tus amigos, utilizando "con copia oculta" o "cco". Aprende cómo en es.tldp.org/Tutoriales/doc-curso-guadalinex-iesaverroes/tema5b.pdf.

*Contar con directrices para el uso de internet en el hogar, reduce en **30 %** la posibilidad de que los niños tengan una experiencia negativa en línea.*

DISCUTIR:

¿Qué información personal es seguro compartir en línea?

5 Gusanos y Barreras

Un miembro del equipo es designado el usuario de la computadora. Otros seis miembros se toman de las manos y forman un círculo alrededor de él/ella. Ellos son el software de seguridad que protege la computadora. Cuatro miembros son el malware que trata de acceder a la computadora. Cuando el líder dice "vamos", el malware intenta tocar al usuario de la computadora mientras que el software de seguridad trata de mantenerlos alejados. Luego, retira a tres o cuatro miembros del software de seguridad, diciendo al grupo que la computadora no ha mantenido su software actualizado. Hagan el juego nuevamente. ¿Es más fácil para el malware alcanzar al usuario de la computadora?

Discutir: ¿Por qué es importante mantener tu software de seguridad funcionando y actualizado? ¿Qué más puedes hacer para proteger tu computadora y la información almacenada en ella?



10 mins

TODAS LAS EDADES



Malware

Malware es el nombre que se da a las herramientas que usan los ciberdelincuentes para dañar la información de tus dispositivos, engañarte para que tomes medidas que no deseas tomar y robar tu información personal. El malware ha existido por más de 25 años, y actualmente se está creando más y más malware para dirigirlo a las redes sociales y teléfonos móviles. Para conocer más sobre algunos tipos comunes de malware, busca spyware, virus informático, caballo de Troya y gusano informático en el glosario.

¿Cómo puedes proteger tu computadora contra el malware?

- Comprueba que tu software de seguridad esté activado y se actualice automáticamente.
- Mantén un cortafuegos (firewall) activado, así como tu software antivirus.

Ten cuidado con el correo spam y los sitios web sospechosos. Si desconfías, no des clic.

¡CONSEJO!

Siempre utiliza un apodo en línea, en lugar de dar tu verdadero nombre, y no des tu verdadero nombre si alguien pregunta.

¿Configuración de tu perfil en una red social o sala de chat? Crea un avatar en lugar de usar tu fotografía.

6 Avatares

Imagina que te estás uniendo a una red social. En lugar de compartir una foto, dibuja un avatar de ti mismo – una imagen de dibujos animados que te represente. Coloca los avatares de todos alrededor del salón de reunión y luego pide a un dirigente que diga los nombres de los miembros del grupo al azar. Todos deben tratar de imaginar qué imagen representa a esa persona, parándose al lado de la misma. Los avatares son una gran manera de expresar tu propia identidad en línea sin revelar tu información a extraños.



15 mins

TODAS LAS EDADES

Llévalo más lejos – Una vez que todos hayan presentado su avatar, pide a uno de los miembros de tu grupo que comience una historia usando su avatar, por ejemplo: ‘Un día muy lluvioso Bjork (el avatar), un duende que vivía pacíficamente en el bosque, escuchó un fuerte golpe en la puerta de su cabaña. Se puso de pie y...’ entonces la siguiente persona continuará la historia introduciendo a su avatar. Dejen volar su imaginación y sean lo más creativos que puedan con su personaje para avanzar en la historia.



10 min

TODAS LAS EDADES

7 Libre de Ser Yo

Las revistas y los anuncios a menudo utilizan la aerografía para crear una imagen de ‘apariencia perfecta’ de los modelos y celebridades. Hagan una tormenta de ideas con el grupo de las diferentes formas en que se utiliza este editor de imagen y luego vean el video ‘Evolución’ de Dove:

www.youtube.com/watch?v=0bozWdKLT6U.

Discutir: ¿Qué tan realista o poco realista es el resultado de la técnica de aerografía (retoque)? ¿Cómo afecta esta imagen de la ‘apariencia perfecta’ creada por los medios, nuestra autoestima y confianza en la apariencia física? ¿Quieres aprender más sobre autoestima y confianza en la apariencia física? Descarga el recurso educativo de la AMGS: [Libre de Ser Yo](http://www.free-being-me.com/es/)



20 mins



computadora/tablet/teléfono
inteligente con acceso a internet,
papel, lápices de colores



Llévalo más lejos – ¡Sé un detective de los medios! Trabaja individualmente o en grupos para encontrar y exponer un ejemplo de imagen de la ‘apariencia perfecta’ que encuentras en los medios de tu sociedad. Imprímela o guárdala en la computadora y escribe por qué no estás de acuerdo con ella. Luego preséntala al resto del grupo.



10 min



computadora/tablet/teléfono
inteligente con acceso a internet.
Opcional: impresora, papel, lápices



8 De un anónimo a otro anónimo

¿Cómo sabes si la persona que conoces en línea es quien dice ser? Elige un personaje favorito de un libro o película y crea lo que tú crees que podría ser su perfil en una red social y la información que podría contener. Crea una versión en papel de ese perfil imaginario, o actúalo – pero no menciones el nombre. Cambien perfiles y trata de adivinar a quién eligió tu amigo. ¿Crees que ahora sabes más sobre esa persona? ¿Puedes confiar en la información que encuentras en un perfil en línea?



15 mins



papel y suficientes lápices de colores para cada participante

ALL AGES

Llévalo más lejos – Imagina que tu amigo va a conocer a esa persona imaginaria a través de una sala de chat, y a ti te preocupa que la persona esté mintiendo sobre su identidad. ¿Qué consejo darías a tu amigo? Imagina las preguntas y las opiniones que podría tener tu amigo, luego escríbele una carta para explicarle tu consejo, o escribe y actúa un diálogo imaginario con un amigo sobre este tema. ¿Cómo crees que podrías ayudar a tu amigo, y es esto diferente a la forma en que podrían ayudarlo sus padres?



15 min



Papel y lápices de colores para cada participante



¡CONSEJO!

Reunirse con un amigo de la web puede ser peligroso. Si realmente se quieren reunir, habla con un adulto de confianza y asegúrate de que te acompañe.

9 Es lo que sabes

En pedazos de papel, todos escriben dos o tres datos sobre una persona imaginaria y los colocan en un recipiente. El grupo se divide en dos equipos y colocan el recipiente lleno en el punto de salida y un recipiente vacío en el punto final. Los recipientes deben estar lo más alejados que sea posible en un área amplia interior o exterior. El Equipo A se reúne en el punto de salida y el Equipo B se esparce por toda el área. A la señal de 'Vamos', cada miembro del Equipo A toma un dato y trata de colocarlo en el recipiente vacío sin ser atrapado. Si es atrapado, el Equipo B toma el dato. El juego continúa con todos los jugadores hasta que los datos están en el recipiente en el punto final o son capturados por el Equipo B. Cuando termina el juego, todos escuchan lo que el Equipo B ha aprendido sobre la persona imaginaria.

Discutir: ¿Y si la persona imaginaria fueras tú, y esos datos fueran información que cualquier persona podría ver en línea? ¿Cómo te sentirías? ¿Qué crees que podría hacer un ciberdelincuente con esa información?



15 mins



papel y suficientes lápices de colores para cada participante

ALL AGES

Se prevé que para el año **2020** más de **50 mil millones** de dispositivos estarán conectados al internet, lo que equivale a siete por cada persona en el planeta.

10 Comparte el aprendizaje

En grupos, organicen una noche informativa sobre la seguridad en internet para un grupo de compañeros o miembros jóvenes de su comunidad, como un grupo de Guías y Guías Scouts más jóvenes. Preparen lo que necesitan saber y planifiquen una serie de actividades divertidas que introduzcan ideas sobre la seguridad en internet sin usar una computadora. Pueden usar las actividades y los juegos de este paquete o crear los propios.



depende de las actividades elegidas para el evento previsto



depende de las actividades elegidas para el evento previsto



Ciberdelincuencia

Ciberdelincuencia es el nombre que se da a las acciones de los criminales en línea. Los delitos cibernéticos son bastante comunes; a nivel mundial, dos terceras partes de los adultos que utilizan el internet han experimentado un delito cibernético

Los tipos de delitos cibernéticos incluyen:

- Dañar tu computadora, eliminando información o dañando el software.
- Robar información privada de tu computadora o red doméstica, como tu dirección de correo electrónico o datos bancarios.
- Convencerte de enviar dinero, a menudo utilizando historias falsas sobre oportunidades de inversión, premios, o que alguien que tú conoces está en problemas en el extranjero y necesita dinero.
- Confirmar tu dirección de correo electrónico para que te puedan enviar más correo basura.
- Usar tu cuenta de correo electrónico (a menudo sin tu conocimiento) para reenviar correo basura y averiguar las direcciones de correo electrónico de tus amigos y familiares.
- Identificarte – con suficiente información personal, los delincuentes cibernéticos pueden aprovecharse de ti en la vida real, por ejemplo, acercándose a ti en un lugar que saben que visitas, o haciéndose pasar por ti en línea.
- Molestando o asustando deliberadamente a alguien.

Recuerda, los delitos cibernéticos son tan ilegales como los delitos que se cometen fuera de línea. Si te encuentras con algo que crees que no es confiable, no respondas - bloquéalo y cuéntaselo a un adulto de confianza.

Cada **60** segundos en Facebook:

510 comentarios se publican,
293,000 estados se actualizan,
136,000 fotos se suben.

¡CONSEJO!

Consulta con un padre/cuidador antes de descargar algo.

Las descargas pueden contener malware que dañaría tu computadora.

11 Envío de correo basura

En grupos, investiguen las principales amenazas de seguridad en internet – malware, phishing y correos fraudulentos. Planifiquen y graben una serie de podcasts cortos informando a la gente sobre estas amenazas y lo que pueden hacer al respecto. Utilicen diferentes formas para hacer el tema interesante y entretenido, como simulacros de entrevistas, mejores consejos y noticias.



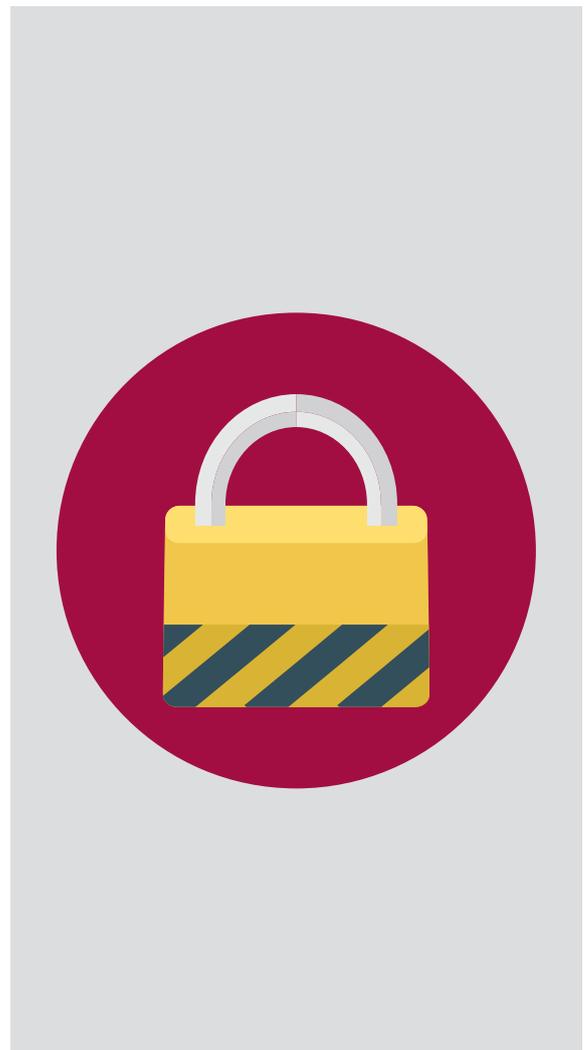
depende de los podcasts



depende de los podcasts



Llévalo más lejos – ¿Por qué no crean una serie de podcasts que puedan subir a una Nube Segura, Archive.org, Ourmedia.org, Podomatic u otros sitios web de podcasts? Asegúrense de verificar que la información que están compartiendo esté correcta y actualizada.



DISCUTIR:

¿Qué tanta información necesita alguien para encontrarte?

12 ¡Phishing!

Phishing es cuando un correo electrónico o sitio web trata de engañarte para que proporciones información privada, como los datos de tus cuentas. Muchos correos de suplantación de identidad (phishing) son atrapados por el filtro de spam en tu cuenta de correo electrónico, pero algunos se escapan y no siempre es fácil identificar la diferencia entre un correo electrónico genuino y un intento de phishing. Entra en línea y haz este juego <http://goo.gl/gdMFFw>.



10 mins



computadora/tablet/teléfono inteligente con acceso a internet



Llévalo más lejos – investiga en línea ejemplos de correos electrónicos fraudulentos, así como las versiones correctas de esos correos e imprímelos – al menos 6 ejemplos diferentes. Al principio, solo muestra los correos fraudulentos en un lugar donde todos los miembros del grupo puedan verlos. Proporciona lápices de colores a cada miembro del grupo y pídeles que coloreen las diferentes partes del correo que parecen sospechosas. Ahora muéstrales los correos reales y compárenlos para comprobar si los comentarios son correctos.



10 min



computadora/tablet/teléfono inteligente con acceso a internet, impresora, lápices de colores



Phishing y correos electrónicos fraudulentos

Los correos electrónicos fraudulentos son mensajes que tratan de convencerte de proporcionar información o enviar dinero a alguien que no conoces. Generalmente cuentan una historia atractiva o dramática y tratan de hacerte reaccionar emocionalmente para que sigas sus instrucciones sin pensarlo.

Phishing es el nombre que se da a una estafa que está tratando de robarte información pretendiendo ser un mensaje de una organización de confianza. El phishing a menudo ocurre por correo electrónico, pero también puedes recibir phishing a través de llamadas telefónicas o mensajes de texto. Los mensajes pueden estar tratando de convencerte de hacer algo dañino como abrir un archivo adjunto que contiene un virus, ir a un sitio web riesgoso, o proporcionar información personal.

Para protegerte de los correos electrónicos fraudulentos y los intentos de phishing, debes estar atento a:

- Correos electrónicos de personas que no conoces o que no estás esperando.
- Correos electrónicos de alguien en tu libreta de direcciones pero escrito de una manera que no suena a tu amigo, o dándote instrucciones que parecen extrañas, como, "He encontrado esta gran oferta" o "haz clic aquí para ver el video".
- Mensajes que no están dirigidos personalmente a ti, por ejemplo, llamándote "Estimado Cliente" en lugar de usar tu nombre.
- Mensajes que utilizan lenguaje dramático o cuentan historias inverosímiles.
- Cualquier correo electrónico que te pide que ingreses tu contraseña o información personal, que verifiques tu cuenta o hagas clic en un enlace.
- Archivos adjuntos que no estabas esperando, o con nombres y tipos de archivos de programas extraños, como los archivos que terminan con ".exe".

Puede ser muy difícil identificar un intento de phishing, así que para mantenerte seguro trata de seguir estas reglas básicas:

- Nunca hagas clic en enlaces de correos electrónicos. En cambio, escribe la dirección del enlace directamente en tu navegador.
- Si sospechas que un correo electrónico puede no ser genuino, no reacciones o respondas. Si dice que viene de un amigo, contáctalo directamente por algún otro medio y comprueba si él envió el correo electrónico.

Si tienes alguna duda, ¡pulsa eliminar!

Respetar...tus derechos y reputación en línea

¡Completa dos de las actividades para ganar tu insignia!

1 Ciberacoso

¿Por qué crees que las personas pueden ser desagradables unas con otras en línea? ¿Cómo sucede y qué podrías hacer para evitarlo? Consulta la definición de ciberacoso (p.41) y pide a tu dirigente que te muestre algunos videos de asesoramiento que exploren lo que es el ciberacoso y cómo evitarlo, luego completa una de las dos actividades siguientes:

DISCUTIR:

¿Se puede rastrear un ciberacoso?

¿Es legal ciberacosar a alguien?

¿Sabrías qué hacer si tú, o un amigo, estuviera experimentando ciberacoso? Usando el consejo en la página 27, prepara una representación para crear conciencia sobre el ciberacoso y recordar a las personas lo que deben hacer al respecto.



la duración de esta actividad varía



computadora/tablet/teléfono inteligente con acceso a internet



Llévalo más lejos – Convierte tu representación en una película sobre el ciberacoso, usando locaciones de tu comunidad. Organiza una fiesta de lanzamiento de tu película y compártela con amigos y familiares.



la duración depende del tipo de encuesta y el informe que quieras hacer



el material depende del tipo de encuesta y el informe que quieras hacer



Lleva a cabo una encuesta sobre el ciberacoso en tu escuela o comunidad para reunir las opiniones y experiencias de tus compañeros. Haz un informe de tus hallazgos, por ejemplo, un cartel que muestre las estadísticas y promueva un comportamiento positivo en línea. ¿Puedes conseguir que tu informe sea publicado por tu escuela y/o comunidad local, ya sea en línea, fuera de línea, o ambos?

Recuerda compartir tus resultados con la AMGS en www.waggs.org/es/internetsafety



depende del tipo de encuesta y el informe que quieras hacer



depende del tipo de encuesta y el informe que quieras hacer

TODAS LAS EDADES



ciberacoso

Cuando alguien utiliza la tecnología para ser deliberada y repetidamente cruel con alguien, eso se llama ciberacoso. A menudo no es con mala intención – simplemente puede ser alguien que está bromeando. Pero si lastima a alguien, eso está mal. Le puede suceder a cualquiera y deja a las personas sintiéndose solas e inseguras. Puede incluir:

- Excluir a las personas de conversaciones en línea.
- Etiquetar imágenes de manera inapropiada.
- Enviar mensajes de texto o correos electrónicos crueles.
- Poner imágenes o mensajes desagradables en los sitios de redes sociales.
- Imitar a otras personas en línea.

A nadie le gusta ser tratado de una manera cruel, ya sea en persona o en línea. El ciberacoso puede ser particularmente molesto porque puede ocurrir en cualquier momento o lugar – logra su objetivo cuando y donde la persona accede a internet o a su teléfono móvil. Si ocurre en un espacio público, como una red social, muchas personas pueden estar involucradas, y la persona que lo inicia puede sentirse en el anonimato – y segura – porque puede ser muy difícil saber en dónde inició una acción cruel.

2 Identifica la diferencia

Un voluntario abandona el salón. El resto del grupo elige un guión y algo que hace al voluntario diferente a ellos, por ejemplo, los miembros del grupo son buzos y el voluntario es una sirena. El grupo comienza a improvisar el guión. El voluntario regresa, se une a la improvisación y trata de averiguar quiénes son los miembros del grupo, y cómo él/ ella es diferente al grupo. El voluntario puede hablar con el grupo y hacer preguntas. Repitan el juego varias veces con diferentes voluntarios y guiones.

Discutir: ¿Cómo se sintió ser diferente? ¿Fue el grupo cordial u hostil? ¿Cómo podrían haberse comportado de una manera diferente? ¿Cómo podría relacionarse esto con tus experiencias en línea?



15 mins



¿Y si me sucede a mí?

- No respondas. Cambia tu configuración de privacidad y bloquea a la persona responsable.
- Si hay un botón de “reportar abuso”, púlsalo
- Guarda copias de los correos electrónicos, textos y conversaciones.
- Encuentra a alguien de confianza, como un buen amigo o miembro de la familia, y háblale al respecto.
- No supongas que nada se puede hacer. El ciberacoso es un delito en muchos países y un acosador a menudo puede ser castigado por la ley.
- Si la persona que está siendo cruel contigo asiste a tu escuela o está compartiendo mensajes crueles con los compañeros de clase, cuéntaselo a un maestro de tu confianza para pedirle consejo. Es posible que la escuela tenga una política y herramientas para ayudarte.

¿Y si le sucede a mi amigo?

Si tienes conocimiento de que alguien está experimentando ciberacoso, tú puedes ayudar.

- No participes. Reenviar mensajes o imágenes desagradables te hace partícipe de un acto aunque tú no lo hayas iniciado.
- Habla con tu amigo y asegúrate de que sepa que lo apoyas y que no está solo.
- Habla con un adulto de tu confianza y reporta lo que está sucediendo.

3 ¡Detén el mensaje!

Coloca a una persona en cada extremo del espacio de reunión. Uno es el emisor y el otro el receptor. Proporciona un objeto pequeño al emisor. Esto representa un mensaje que está siendo publicado en línea. El resto del grupo se divide en dos equipos. Un equipo intenta llevar el mensaje de un extremo a otro del salón, pasándolo en secreto entre el mayor número posible de miembros del equipo. El otro equipo trata de identificar quién tiene el mensaje e intenta detenerlo, tocando en el hombro a la persona que sostiene el objeto. Promueve diferentes estrategias, como velocidad y esquivar, perspicacia y secreto, o distraer al equipo rastreador.

Discuss: Los mensajes pueden difundirse muy rápidamente en línea. ¿Qué crees que puedes hacer para asegurarte de que tus mensajes en línea no tengan consecuencias negativas?



15 mins



objeto pequeño, como una pelota de ping-pong



Llévalo más lejos – Trabajen en parejas para elaborar una lista de los criterios que deben considerar cuando publican algo en línea. Den alrededor de 10 minutos a cada grupo para que trabaje en su lista y luego retroalimente al resto del grupo. Pide a alguien que tome nota de todos los criterios en un pedazo de papel y pide al grupo que vote por las 5 cosas importantes que se tienen que considerar al publicar un mensaje en línea.



15 min



papel y lápiz para cada participante



DISCUTIR:

¿Cómo sabes que alguien es quien dice ser?

4 ciberamigos

Tener buenos amigos es importante para todos. ¿Cómo puedes ser un buen amigo en tu vida diaria y en el internet?

Discutir: ¿Cómo puede afectar a tus amistades en la vida diaria, la forma en que tratas a tus amigos en línea? Piensa en tres formas simples de ser un buen amigo en línea y luego crea una imagen mostrando tus ideas, como una promesa que haces a tus amigos. Intercambien las promesas en su grupo y exhibe la promesa de tu amigo en casa.



10 mins



papel y lápices de colores para cada participante



Llévalo más lejos – Una vez al día durante la próxima semana, haz un esfuerzo por publicar un mensaje positivo en línea, con el fin de que los demás se sientan bien consigo mismos, como parte de tus actividades regulares en las redes sociales.



una semana



computadora/tablet/teléfono inteligente con acceso a internet





5 ¿Anónimo en línea?

Reúne nuevas historias sobre la censura y el anonimato en línea. ¿Cuándo ser anónimo en línea es una buena idea, y cuándo puede ser una mala idea? ¿Crees que está bien que el contenido en línea sea censurado (ocultado de las personas)? Divídanse en dos equipos, uno representa el argumento para la censura y el otro grupo el argumento en contra. Den algún tiempo para que los grupos discutan y acuerden 3 puntos clave para este tema. Luego retroalimenten al resto del grupo.



20 mins



suficiente papel y lápices para cada participante

TODAS LAS EDADES

Llévalo más lejos – Usando los puntos clave de la actividad anterior y con alguna investigación adicional planifica un debate sobre la censura o el anonimato en línea, un grupo hablará “a favor” y el otro “en contra”. Investiga tu caso y organiza el debate, invita a tus amigos y familiares a asistir.



depende del tipo de encuesta y el informe que te gustaría hacer



depende del tipo de encuesta y el informe que te gustaría hacer

+13



Conoce tus huellas

Es fácil pensar que permaneces en el anonimato cuando estás en línea, pero no es así. Cada vez que entras en línea dejas un rastro. Eso no es necesariamente malo, si la información sobre ti es positiva y no revela ninguna información privada. Cualquier cosa que tú u otros publican sobre ti se agrega a tu “huella digital”.

Estos son algunos consejos para ayudarte a entender la marca que estás haciendo en el internet.

- Haz una búsqueda de vanidad, escribiendo tu nombre en Google y viendo los resultados. Si hay muchas personas con tu mismo nombre, intenta agregando palabras, como el país o la ciudad donde vives.
- Mira la sección del historial de tu navegador para ver los sitios web que has visitado en el pasado.
- A cada dispositivo en línea se le asigna un número especial para identificarlo cuando está conectado al internet. Esta es la dirección IP. Si es necesario, los sitios web y organizaciones como la policía pueden utilizar la dirección IP para identificar quién ha realizado una determinada acción en línea.
- Nada de lo que subes a la web puede ser realmente eliminado para siempre. Las personas que quieren saber más sobre ti, ¡pueden averiguar mucho buscándote en el internet – ¡así que ten cuidado con lo que compartes!

Si no te gusta lo que encuentras, primero ve si puedes eliminar algo del contenido, pero recuerda que aunque elimines esa publicación o fotografía vergonzosa, nunca puedes estar seguro de que realmente ha sido borrada del internet. Tu próximo paso debe ser crear contenido positivo sobre ti mismo en línea, contenido seguro que no revele nada personal sobre ti y te presente de una manera positiva, de modo que puedas favorecer resultados positivos de búsqueda que te impulsarán hacia lo más alto de Google.



6 ¿Cuál es el patrón?

Un voluntario abandona el salón, y el resto del grupo se sienta en un círculo y elige a una persona para iniciar una acción, como aplaudir, tocar su cabeza o dar una palmada en sus rodillas. Esta persona puede cambiar la acción en cualquier momento, y los otros deben seguirla. Se vuelve a llamar al voluntario, quien se parará en el centro del círculo, y tratará de identificar a la persona que está cambiando la acción. Tiene dos oportunidades para descubrirlo. Hagan este juego unas cuantas veces.

Discutir: ¿Qué tan fácil es identificar a la persona responsable de cambiar la acción? ¿Qué tan difícil sería identificar a una persona responsable de iniciar un rumor o enviar un mensaje en línea? ¿Sería más fácil averiguar de dónde provino el mensaje si nadie copiara a la persona que está cambiando la acción y difundiendo un mensaje?



10 mins



DISCUTIR:

¿Compartir archivos de música en línea puede permitir que otros tengan acceso a tu computadora?

7 Buena reputación

Tu reputación digital es la imagen en línea que presentas a través de tus acciones en línea. Esto incluye las fotos que subes, los posts que escribes, los correos electrónicos o mensajes que envías y los comentarios que haces en las salas de chat, servicios de mensajería, foros o sitios web.

Imagina que estás solicitando un empleo o aplicando para un curso. Escribe cinco cosas que te gustaría decir acerca de ti mismo en tu solicitud. Luego ve tu perfil en las redes sociales y busca tu nombre en internet. ¿Cuáles crees que son las tres cosas principales que dirán tus perfiles en línea acerca de ti? ¿Qué puedes hacer para estar seguro de que la persona que te está ofreciendo el empleo o curso vea lo que tú quieres que vea si hace una búsqueda de tu nombre en internet?



10 mins



computadora/tablet/teléfono inteligente con acceso a internet, papel y un lápiz para cada participante





Reputación digital

No tengas remordimientos. Esa broma que mandaste sobre tu maestra/o... ¿cómo te sentirías cuando de pronto apareciera en su escritorio? O esa foto donde estás de fiesta – dentro de cinco años – ¿es lo que quieres que vea tu nuevo jefe cuando busque tu nombre en línea? Tu reputación digital es lo que otros piensan de ti a través de tus acciones en línea, y a diferencia de algo que puedes decir en voz alta, el internet no olvida las cosas que publicas. ¿Cómo quieres que te vea la gente? Tal vez no te des cuenta, pero tú tienes el control. Estos son algunos consejos para mantener una reputación digital favorable:

- Comprueba tu configuración de privacidad en las redes sociales para evitar que extraños encuentren información sobre ti.
- Sé positivo, evita lo negativo. Considera lo que alguien que respeta podría pensar si viera tu publicación o fotografía.
- Si un amigo te etiqueta en una foto que te retrata de una manera negativa, elimina la etiqueta y pide a tu amigo que retire la foto.
- Cuando configures tu perfil en una red social, no utilices tu nombre completo.
- Verifica tu ortografía y gramática. Algunas empresas consideran los errores de ortografía y gramática como un signo de inmadurez y malas habilidades de comunicación.
- Recuerda que la publicación es permanente, así que siempre piénsalo dos veces antes de poner algo en línea.
- Monitorea tu reputación digital, buscando tu nombre en línea, y pide que se retire cualquier cosa que no quieres que aparezca en línea.
- Si quieres retirar algo de tu Sistema, habla con alguien cara a cara.

Si lo arruinas, actúa rápidamente para arreglar las cosas. La información viaja tan rápido, que si quieres limitar las consecuencias de esa publicación desagradable o foto vergonzosa, tienes que eliminarla lo más rápido que puedas. ¿Le debes una disculpa a alguien? Quedas mucho mejor si asumes la responsabilidad por tus errores.



8 Estudia inteligentemente

¿Estás luchando con un trabajo escolar o estás retrasado en una tarea? Puede ser muy tentador buscar información sobre la materia en el internet y copiarla y pegarla en tu trabajo. El problema, tus maestros pueden detectar fácilmente lo que has hecho y utilizar el internet para rastrear el sitio donde encontraste el texto.

Haz la prueba. Trabajando en parejas, una persona encuentra unos cuantos párrafos de texto en línea, los copia y los pega en un documento de Word y lo envía por correo electrónico a otra persona, que trata de rastrear su fuente.



10 mins



computadora/tablet/teléfono inteligente con acceso a internet



Los **primeros mil millones** de usuarios de internet se alcanzaron en **2005**. Los **segundos mil millones** en **2010**. Los **terceros mil millones** en **2014**.

¡CONSEJO!

Establece límites cuando juegas en línea y utiliza una alarma.

9 Acorta la distancia

Cuando enfrentas un problema en línea, a menudo se te aconsejará hablar con un adulto de confianza, como un padre/cuidador, maestro, o líder de grupo comunitario. Sin embargo, tal vez no quieras hacerlo. En grupos pequeños, hagan una tormenta de ideas de los problemas en línea que han oído hablar o han experimentado, y decidan qué problemas deben informar a un adulto o cuándo sería útil el apoyo de un adulto



15 mins



papel y lápiz

TODAS LAS EDADES

Llévalo más lejos – ¿Te sientes cómodo hablando con tus padres/cuidadores sobre lo que haces en línea? Piensa en una acción que podrías tomar que podría ayudarte a ti y tus padres/cuidadores a hablar más abiertamente sobre tu uso del internet, por ejemplo, darles un recorrido de tus sitios web favoritos, enseñarles cómo hacer algo en línea, o encontrar un acuerdo de uso del internet que ambos puedan firmar.



15 mins



papel y lápiz

TODAS LAS EDADES

10 Tiempo en línea

¿Cuánto tiempo crees que pasas en línea cada semana? Haz una lista de las principales actividades que realizas en línea, como ver tus correos electrónicos, chatear con amigos en línea, streaming de música, jugar juegos o usar las redes sociales. Junto a cada actividad, anota cuántas horas y minutos crees que le dedicas cada semana. En la siguiente semana, lleva un registro del tiempo que pasas en cada uno de los elementos de tu lista, y compáralos con tus estimaciones. ¿Hay alguna diferencia? ¿Cuánto tiempo crees que debes pasar en línea cada semana?



una semana



computadora/tablet/teléfono inteligente con acceso a internet, papel y un lápiz



Llévalo más lejos – Con tu grupo, hagan un reloj con la carátula en blanco y manecillas móviles. Con tus padres/cuidadores acuerden cuánto tiempo es conveniente pasar en línea cada semana, y marquen este número de horas en el reloj. Al inicio de la semana, pongan el reloj en "0".



5min y luego depende de la investigación



computadora/tablet/teléfono inteligente con acceso a internet, papel y lápiz



¡CONSEJO!

Piensa antes de publicar – una vez que haces clic en “enviar”, estará por allí para siempre, y tú no podrás controlar quién lo ve. Incluso si lo eliminas después, alguien podría haberlo guardado.

11 Huella digital

¿Tienes idea de cuánto contenido pones en línea? Dibuja el contorno de una gran huella en un pedazo de papel y, durante la semana, cada vez que publiques o subas algo a la web, anótalo en tu huella - no pongas exactamente lo que dijiste, sólo descríbelo, por ejemplo, “actualicé mi estado”, “chateé con Raúl durante media hora en Messenger”, subí a Facebook 20 fotos de la fiesta de mi cumpleaños. Compartan sus huellas digitales en su lugar de reunión. ¿Cuánto tiempo te tomó llenar tu huella? Imagina cuántas huellas llenarías en un año y cómo te haría sentir.



10 mins



computadora/tablet/teléfono inteligente con acceso a internet, papel y un lápiz

TODAS LAS EDADES

Llévalo más lejos – Visita el sitio web www.internetlvestats.com y registra cuántos tuits, fotos y publicaciones de Facebook se suben cada segundo al internet. También puedes ver la emisión diaria de CO2 del internet. ¿Cómo te sientes al ver estos números cambiando tan rápidamente? Investiga en línea acerca de la ecología y el internet, y trata de hacer una infografía para presentar tus hallazgos a tu grupo.



5min y luego depende de la investigación



computadora/tablet/teléfono inteligente con acceso a internet

TODAS LAS EDADES



En el mapa

¿Te has preguntado cómo puede funcionar un teléfono móvil fuera de tu ubicación en un mapa?

Los servicios de localización son realmente útiles. Te pueden decir dónde se encuentra la parada de autobús o cajero más cercano, te ayudan cuando estás perdido, y si estás en problemas, los servicios de emergencia pueden usar la señal de tu dispositivo móvil para encontrarte. Si pierdes tu aparato, incluso puedes utilizar la señal para rastrearlo. Pero otras personas también pueden utilizar los servicios de localización para encontrarte, y podrían ser personas que no conoces o en quien no confías.

Así que, ¿Cómo funciona? Hay tres maneras principales de localizar un teléfono móvil (encontrarás más información en el glosario):

- Sistema de Posicionamiento Global (GPS por sus siglas en inglés) que recibe señales de los satélites que orbitan la tierra.
- Sistema Global de Comunicaciones Móviles (GSM por sus siglas en inglés) que funciona de forma similar pero utiliza las señales enviadas desde antenas de telefonía en lugar de satélites.
- Por último, tu dispositivo puede ser localizado viendo los puntos de acceso a internet inalámbrico, como la red inalámbrica de tu casa o las zonas de cobertura inalámbrica (Wi-Fi) con las que puede comunicarse tu dispositivo.

Si tienes un teléfono con internet, probablemente utiliza los tres métodos combinados para señalar tu ubicación de una manera rápida y precisa. Una vez que tu dispositivo proporciona tu ubicación, hay muchas maneras de compartirla en línea. Sin embargo, tú no puedes controlar quién ve esta información, así que es una mala idea permitir que los extraños sepan en dónde estás, cuando tú no sabes quiénes son. Piénsalo bien antes de utilizar los servicios de localización, especialmente si lo hacen público

¡CONSEJO!

¿Quieres probar lo que has aprendido? Intenta jugar el juego cuida tu IMAGEN on line : www.cuidatuimagenonline.com

12 Descarga consciente

Hay una gran cantidad de contenido digital fantástico en línea que puedes descargar, como fotos, música y películas, así como aplicaciones para tu teléfono móvil y tablet, pero es importante verificar que estás utilizando sitios legales y no estás tomando nada protegido por derechos de autor sin pagar por ello. Descargar archivos ilegales se llama piratería.

En grupos, imaginen que son cantantes cuya música ha sido robada a través de la piratería en línea. Escriban una canción o mensaje de rap para las personas que robaron su música, explíquenles cómo los hacer sentir esto.



20 mins



papel y lápiz

ALL AGES

Llévalo más lejos – Graben su actuación y súbanla al canal de YouTube de la AMGS. Recuerden verificar que todos los involucrados están contentos de aparecer en línea.



20 mins



cámara/tablet/teléfono inteligente con acceso a internet

ALL AGES



¿Es correcto descargar?

Streaming y descargar medios como películas y música es una gran parte de la actividad en línea, y hay un montón de sitios web que te dan acceso fácil a material nuevo increíble. Lamentablemente, esto no siempre es legal. Esto tiene que ver con los derechos de autor. Si tú creas algo original, tú eres el dueño y tienes derecho a controlar quiénes lo utilizan, cambian o copian. Los artistas ganan a través de las regalías, que es el dinero que les pagan cada vez que alguien compra una copia de su trabajo – ya sea que se trate de un CD/DVD, boletos para un concierto o proyección de una película, o una versión digital. Si descargas algo ilegalmente, te estás llevando una copia sin el permiso del propietario.

Así que tienes que tomar una decisión. ¿Dónde obtienes tus descargas y qué significará esa decisión para ti?

Algunos puntos para reflexionar:

- El riesgo de recibir malware en tu computadora es mucho mayor si descargas archivos ilegales.
- Es cierto que las empresas que manejan a los artistas, como las firmas disqueras, a menudo ganan mucho más que los propios artistas. Sin embargo, estos son acuerdos entre los artistas y las empresas, y no tienen que ver con nuestras decisiones en torno a pagar por el contenido que queremos, o tratamos de obtener gratuitamente.
- A muchos artistas les molesta pensar que lo que les costó tanto trabajo crear pueda conseguirse por nada. Cuando las personas descargan copias piratas del trabajo de un artista, no consideran cómo se siente el creador al respecto.
- Si usas servicios ilegales, estás violando la ley. Tal vez piensas que la posibilidad de ser atrapado es realmente pequeña, pero si eres alguno de los que son atrapados y acusados, las consecuencias pueden ser muy grandes: multas enormes, prohibiciones en internet, un registro criminal, incluso un tiempo en la cárcel. Es algo que realmente podría afectar tu futuro.
- Algunas personas dicen que copiar algo no es lo mismo que robarlo, porque en realidad no se lo han quitado a alguien. Pero es como decir que una canción o película no es un producto que compramos. Si eso fuera verdad, ya no habría nuevas canciones o películas, porque los artistas y las industrias que los rodean no podrían tener ganancias.
- Las copias piratas a menudo son de calidad muy inferior a lo que compras legalmente.
- Esto no significa que tendrás que pagar una fortuna para obtener música o ver películas. Hay muchas maneras de obtener contenido de manera legal, y no todo cuesta dinero.

¡Ponerte en Primer Lugar!

¡Debes hacer esta actividad para ganar tu insignia!

Ahora que tienes una buena idea sobre cómo sacar el mayor provecho del internet y al mismo tiempo mantenerte seguro, detente y piensa en lo que has aprendido. ¿Cómo puedes poner en práctica estas ideas en tu propia vida? Imagina que te estás haciendo una promesa a ti mismo para mantenerte seguro en línea. ¿Qué dirías?



Por ejemplo...

“Me voy a detener a pensar antes de publicar información en internet.”

“Voy a hablar con un adulto de confianza si sucede algo en línea que no me gusta.”

“Voy a tener cuidado al abrir correos electrónicos o enlaces y bloquearé cualquier cosa que me parezca insegura”

Elige tus principales promesas y escríbelas en el siguiente cuadro. Imprime el cuadro y compártelo con tu familia. Colócalo cerca de tu computadora donde puedas verlo para ayudarte a recordar lo que has aprendido.

Mi Promesa de Seguridad en el Internet

Quiero estar seguro en línea, cuidar a mis amigos y ser capaz de disfrutar el uso del internet.

Para que esto suceda, me prometo que trataré de...

-
-
-
-
-

Firma..... Fecha.....

¡Comparte!

¡Comparte tu experiencia Surf Smart, las fotos que tomaste y los videos que creaste, con las Guías y Guías Scouts de todo el mundo!

¡Hay muchas maneras de conectarte con la AMGS!



Visita www.waggs.org



Twitter (@waggs_world)



Facebook
(www.facebook.com/waggs)



Dinos qué piensas del paquete de actividades, completando la encuesta en línea:

www.waggs.org/es/internetsafety



Envía un correo electrónico con tu historia Surf Smart a youthlearning@waggs.org

Notas

Directrices de seguridad en internet para adultos

Estas directrices están dirigidas a padres, tutores y dirigentes de Guías/Guías Scouts, y tienen como objetivo ayudarlos a entender cómo pueden proteger mejor la seguridad y la privacidad de los jóvenes a su cuidado. Ciertos puntos serán requisitos legales en algunos países pero no en otros, aunque se pueden considerar mejores prácticas incluso si no son legalmente vinculantes.

Considera la forma en que proteges a los niños en la vida real. Tienes cuidado de mantenerlos alejados de situaciones físicas peligrosas. Monitoreas en dónde se encuentran, con quiénes están, qué ven, y cómo se comportan. Ahora aplica esos mismos criterios al internet y sus interacciones digitales y piensa cómo puedes minimizar los daños y asegurar que los niños estén protegidos y seguros. Como dirigente de jóvenes, debes tener cuidado de auto-regular tus actividades en línea y evitar que tu mundo privado y tu mundo público se sobrepongan.

Política de correo electrónico

- Crea un sistema de correo electrónico para tu grupo. Selecciona a un voluntario adulto para que sea responsable de agregar, editar y eliminar direcciones de correo electrónico del sistema. Crea listas de correo para padres/cuidadores, miembros de cada grupo de edad y dirigentes de grupo.
- Utiliza la función “con copia oculta” (cco) cuando envíes correos electrónicos a grupos, para proteger a todos y evitar el spam.
- Mantén la lista únicamente para la comunicación con el grupo de Guías/Guías Scouts. No reenvíes cadenas de correos electrónicos a jóvenes. No compartas la lista con quienes no son miembros.
- Evita la comunicación privada directa con niños, distinta a los mensajes genéricos del grupo.
- Si quieres contactar a alguien menor de 16 años utilizando un correo electrónico o texto, debes tener un permiso escrito de sus padres/cuidadores. Copia a otro adulto en cualquier mensaje que envíes a un miembro menor de 18 años.
- En caso de que un niño tenga que contactarte directamente a ti o a otro dirigente adulto, discute con otros voluntarios adultos la mejor manera de manejar esta situación. Dependiendo de la naturaleza de la comunicación, considera si los padres/cuidadores del niño deben ser notificados. Tu respuesta puede variar de acuerdo a la edad del niño: un miembro mayor del grupo de Guías/Guías Scouts puede interactuar con los dirigentes del grupo, aunque los padres/cuidadores deben ser informados de esto cuando el niño se une al grupo.
- Examina el contenido de tu mensaje, comprobando que el lenguaje e imágenes sean apropiados para la edad del grupo, y comprueba a dónde conducen los enlaces.

Política de las redes sociales

- Si la creación de una red social beneficiará a tu grupo, asegúrate de que el grupo sea privado.
- Invita a miembros del grupo de una edad apropiada, y a sus padres, a unirse a la página o sitio de la red social del grupo. Ten en cuenta que las redes sociales tienen diferentes políticas de edad, por ejemplo, los miembros menores de 13 años no deben tener una cuenta de Facebook o utilizar YouTube. Utiliza configuraciones estrictas de privacidad para evitar que las publicaciones y las fotos sean vistas por quienes no son miembros de tu grupo. Cuando un miembro se vaya, asigna a un voluntario adulto la responsabilidad de eliminar al miembro y a sus padres/cuidadores del grupo.
- Crea una política en cuanto a si los adultos y miembros jóvenes pueden aceptarse entre sí como amigos en las redes sociales. Busca el consentimiento de los padres antes de aceptar en línea la ‘amistad’ de un niño.
- Define tu responsabilidad y las acciones apropiadas que deben tomarse en caso de observar que un miembro joven hace publicaciones con malas palabras, imágenes inapropiadas o enlaces a contenido inapropiado.
- Evita la comunicación privada directa con niños, que no sean los mensajes genéricos del grupo. En caso de que un niño tenga que contactarte a ti o a otro dirigente adulto, discute con otros voluntarios adultos cómo manejar esta situación (ver la política de correo electrónico anterior).

Política de fotos y video

- Crea una política para tu grupo en cuanto a si se tomarán o no fotos de las actividades del grupo, y obtén el consentimiento firmado de los padres/cuidadores para esta política antes de tomar una foto a su hijo. Incluye información acerca de si se compartirán o no las fotos con los miembros del grupo y sus padres. Aunque a la mayoría de los padres les gustará tener esas fotos y videos como recuerdo, algunos pueden oponerse a que se tomen y/o compartan fotos de su hijo por razones religiosas, de privacidad u otras. Si los padres optan por no compartir las fotos, debes tener en cuenta que sus hijos no deben ser fotografiados cuando se tomen fotos y videos.
- Si configuraste páginas en línea para compartir fotos y videos, éstas deben ser privadas y de preferencia estar protegidas por una contraseña. Obtén el consentimiento de cualquier persona que aparezca en las fotos/videos antes de subirlos a la red.
- Haz un alto y piensa antes de compartir fotos o videos de jóvenes en línea o nombrar personas en imágenes a través de "etiquetar". Si deseas compartir este contenido, asegúrate de tener el permiso escrito de sus padres/cuidadores antes de hacerlo.

Seguridad general en línea

- **Asegura tu propia computadora y otros dispositivos:** Asegúrate de que tu computadora y otros dispositivos habilitados con internet estén asegurados contra virus y malware mediante el uso de software de seguridad en internet, y estando alerta a los escaneos en busca de malware. De esta manera puedes prevenir la propagación de malware a otros miembros del grupo, o el acceso no autorizado a los datos privados de los miembros y la información financiera almacenada en tu computadora u otros dispositivos.
- **Utiliza contraseñas para proteger tus dispositivos:** Los niños pueden pedir prestado o utilizar el teléfono, cámara digital, tablet o computadora de un voluntario adulto. Tú puedes impedirles el acceso a archivos o programas específicos mediante el uso de contraseñas, siempre que sea posible. Asegúrate de que no haya material objetable almacenado en tu dispositivo – si lo hay, puedes estar seguro de que un niño lo encontrará. Una contraseña también puede impedir que un niño compre música o apps sin tu permiso.
- **Banca en línea:** Se pedirá que el tesorero de tu grupo asegure su computadora con software de seguridad en internet y monitoree cuidadosamente quiénes pueden tener acceso a la cuenta bancaria del grupo, ya sea físicamente o en línea. Evita realizar transacciones financieras en computadoras públicas o en redes inalámbricas públicas que podrían tener una configuración de seguridad inferior que tu red personal. Consulta la cuenta en línea por lo menos una vez a la semana para verificar que todas las transacciones estén autorizadas. Inmediatamente reporta a tu banco cualquier actividad extraña para minimizar las pérdidas en la cuenta.
- **Almacenamiento de los registros de los miembros:** ¿Quién guarda los formularios de los registros privados de tu grupo? Si estos incluyen nombres, números telefónicos, direcciones de casa y correo electrónico, datos de seguros médicos y enlaces a bases de datos, podrían ser material valioso para un ladrón de identidad. Establece normas para almacenar y proteger las copias físicas y digitalizadas de estos formularios.

Proteger a los miembros del grupo

- Si un joven te ha confiado que piensa reunirse con alguien que conoció en línea, asegúrate de que lo sepan sus padres/cuidadores. Recomienda que si los padres/cuidadores permiten la reunión, deben acompañar a su hijo y asegurarse de que el encuentro sea en un lugar público. Aunque muchas personas entablan nuevas amistades genuinas en línea, existen preocupaciones justificadas para reunirse con alguien sin haber podido comprobar primero que esa persona es quien dice ser.
- Si te das cuenta de que un niño bajo tu supervisión está involucrado en actividades en línea potencialmente peligrosas, como visitar un sitio para adultos u otros sitios inapropiados, utilizar un archivo ilegal, compartir dispositivos, o unirse a grupos en las redes sociales que promueven un comportamiento anti-social, debes determinar sus responsabilidades con los niños, sus padres/cuidadores y la comunidad y actuar en consecuencia. Discute el mejor curso de acción con otros dirigentes adultos. No te de miedo 'dar la señal de alarma' y alertar a los padres/cuidadores de los riesgos y peligros potenciales.

Recursos

Seguridad en Internet

Juego en línea de Childnet International: www.kidsmart.org.uk

Sitio web de Childnet International: www.childnet-int.org

Informe EU Kids Online: www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Información de privacidad de Facebook: www.facebook.com/help/privacy

Alianza Nacional de Seguridad Cibernética: staysafeonline.org/

Taller NetSmartz: www.netsmartz.org

Sé Dueño de tu Espacio – Libro electrónico para adolescentes
www.microsoft.com/download/en/details.aspx?id=1522.

Centro de Seguridad por Google: www.google.co.uk/goodtoknow

Día Internacional del Internet Seguro – una iniciativa del proyecto EU SafeBorders: www.saferinternetday.org

Think You know (Piensas que Sabes): www.thinkuknow.co.uk

Videos que muestran cómo verificar algunas opciones fundamentales de privacidad y seguridad:
www.kidsmart.org.uk/skills-school/

Aprendizaje y oportunidades

Sitio web de la AMGS: www.wagggg.org

Red de organizaciones juveniles de Europa: www.eurodesk.org.uk

Consejo de Europa: www.coe.int/t/dg4/youth/default_en.asp

Pláticas inspiradoras sobre diversos temas: www.ted.com/

Descubre cómo las cosas funcionan de manera diferente: www.howstuffworks.com

Instituto cultural Google: www.googleartproject.com

Agencia de la ONU enfocada en cuestiones de género: www.unwomen.org

Juventud Europea en acción: www.youthforum.org

Codificación y programación para niños y jóvenes: www.code.org/frozen

Ambientes de Aprendizaje Auto-organizados: www.theschoolinthecloud.org

Sitio de la BBC sobre tecnología:
www.bbc.co.uk/webwise/ ¿Interesado en la codificación? Prueba: <http://studio.code.org/>

Glosario

Aerografía - para alterar (una imagen, especialmente una fotografía) utilizando software para editar fotografías u otras técnicas para aumentar su atractivo u ocultar la parte no deseada.

Almacenamiento en la nube – un servicio que permite a los usuarios guardar información mediante la transferencia de la misma a través de internet a un sistema de almacenamiento externo mantenido por un tercero.

Ancho de banda – la máxima cantidad de información que puede transmitirse a través de un canal, como una conexión a internet.

Antivirus – software que está diseñado para detectar y destruir virus informáticos.

Avatar – Imágenes gráficas usadas para representar usuarios en espacios en línea; pueden ser o no representaciones auténticas de las personas que las utilizan.

Blogging – Compartir nuestras opiniones y experiencias en la forma de un diario en línea donde los lectores pueden comentar las publicaciones.

Caballo de Troya – es como un virus, excepto que está diseñado para pretender que va a hacer algo que uno quiere que haga, luego secretamente lleva a cabo una acción no deseada, como copiarse a sí mismo, dar a alguien acceso a nuestra computadora o robar información. Un ejemplo puede ser un juego o protector de pantalla gratuito. Uno descarga el archivo sin darse cuenta de que tiene una pieza de malware oculta en el interior.

Ciberacoso - el uso de información y tecnologías de comunicación para respaldar un comportamiento deliberado, repetido y hostil de una persona o grupo que tiene la intención de dañar a otros.

Ciberdelincuencia – cualquier delito que involucra una computadora y una red.

Código QR – un código de barras móvil legible por dispositivos móviles, con una cámara que dirige al usuario a un sitio web cuando se escanea.

Descargar – transferir un archivo o programa de un sistema remoto a una computadora local o dispositivo móvil.

Etiquetado – identificar a alguien que aparece en una foto o video en línea, adjuntado una etiqueta de nombre virtual, o “tag”.

Facebook – la red social más grande en internet. Permite a los usuarios crear perfiles personales y hacer conexiones con sus amigos.

Geo data (datos geográficos) – datos digitales que representan una localización geográfica.

- **GPS (Sistema de Posicionamiento Global)** – un sistema de navegación que utiliza satélites y computadoras para calcular la localización del dispositivo receptor. Muchos teléfonos móviles contienen receptores GPS. Si nuestro teléfono tiene un receptor GPS, puede recibir señales de satélites que orbitan la tierra. Los satélites envían señales y el GPS usa la distancia entre los satélites y el receptor (nuestro teléfono) para calcular dónde se encuentra uno.
- **GSM (Sistema Global para Comunicaciones Móviles)** – una norma para comunicaciones móviles utilizado por la mayoría de los servicios de telefonía móvil en el mundo. También puede ser utilizado para identificar la ubicación de un dispositivo móvil en relación a las antenas de telefonía móvil que transmiten a ese dispositivo.

Gusano informático – un tipo de virus que puede viajar de una computadora a otra por sí mismo. Se puede copiar a sí mismo y enviar cientos de miles de copias, por ejemplo, a todos los que figuran en nuestra libreta de direcciones de correo electrónico. Los gusanos pueden ser diseñados para dar acceso a los cibercriminales y permitirles controlar nuestra computadora de forma remota, pero lo más común es que sólo utilizan la memoria del sistema o el ancho de banda de la red, dañando las computadoras y los servidores de internet.

Huella digital – la suma del rastro de información que dejan las personas en línea.

Malware – software destinado a dañar o averiar computadoras y sistemas informáticos. El Malware incluye spyware, virus, caballos de Troya y gusanos informáticos.

Marca de agua digital – un patrón insertado en un archivo digital de imagen, audio o video que contiene información de los derechos de autor del archivo, tales como autor y derechos.

Phishing – se refiere a comunicaciones fraudulentas que tratan de obtener información personal, como nombres de usuarios, contraseñas y datos de tarjetas de crédito, mediante el envío de mensajes, ya sea en línea o a través del teléfono, que pretenden ser de una organización legítima.

Piratería en internet – cargar o descargar ilegalmente material con derechos de autor a través de internet.

Podcast – una serie de archivos digitales de medios de comunicación, ya sea audio o video, que son liberados en fragmentos y son descargados o escuchados en línea.

Reputación digital – lo que las personas piensan de uno en base a nuestra información visible en línea.

Servicios de localización – un servicio que proporciona la localización de un dispositivo en el mundo fuera de línea, ya sea móvil o fijo.

SKYPE – un programa informático muy popular que permite a los usuarios crear perfiles, hacer llamadas telefónicas gratuitas, chat y video chat a través de su computadora o dispositivo móvil desde cualquier lugar del mundo.

Software de seguridad – software que protege una computadora contra una serie de amenazas.

Spyware – un tipo de software malicioso que se instala a sí mismo en una computadora y reúne información sin nuestro conocimiento. Es difícil averiguar si hay un spyware instalado en nuestra computadora, por lo que es importante tener un buen software de seguridad para protegernos.

Streaming – una manera de enviar información a través de una red informática como un flujo regular y constante, permitiendo que el contenido se reproduzca mientras se está recibiendo el resto de la información.

Twitter – un servicio de red social que permite a los usuarios enviar y leer los mensajes, o tuits, de otros usuarios de hasta 140 caracteres de longitud.

Etiquetado – identificar a alguien que aparece en una foto o video en línea, adjuntando una etiqueta “tag” de nombre virtual.

Virus informático – un programa que puede copiarse a sí mismo y propagarse de una computadora a otra, dañando la información almacenada en la computadora e impidiendo su correcto funcionamiento.



Este proyecto ha sido posible en parte por una subvención de la Fundación Symantec, un fondo corporativo designado de Silicon Valley Community Foundation.

Symantec fue fundada en 1982 por visionarios expertos en informática y la empresa ha evolucionado hasta convertirse en una de las empresas de software más grandes del mundo. Ofrece seguridad, almacenamiento y soluciones de gestión de sistemas a los clientes – desde consumidores y negocios pequeños hasta las más grandes organizaciones globales. Su Sede Central está en California, E.E.U.U.

Silicon Valley Community Foundation ofrece liderazgo comunitario visionario, identificando los desafíos emergentes y abordando esos desafíos a través de sus programas de otorgamiento de subvenciones e investigación. También tiene su sede en California, E.E.U.U.



