CIBERSEGURIDAD:
Tu reto diario

Recomendaciones para el correcto uso de internet para jóvenes en edad escolar

Líderes 2.0 | lacnic

"Bloquear y restringir sitios web no hace nada bueno para los estudiantes a largo plazo, pero enseñarles cómo estar seguros en línea les permite practicar buenos hábitos durante toda su vida. Internet es una de las mejores herramientas del planeta para mejorar el aprendizaje de los estudiantes. Es un montón de información esperando a ser devorado por mentes hambrientas. Sin embargo, también puede ser un lugar peligroso donde los estudiantes se encuentran solos y sin educación acerca de cómo manejar situaciones difíciles."

Robert Lucas.

Instrucciones para la charla

Este guion se ha desarrollado para servir como referencia a quienes utilicen la presentación ¡CIBERSEGURIDAD: tu reto diario! (diseñada para jóvenes entre 13 y 18 años). También podría adecuarse el material para niños menores si así se requiere.

Los textos que aparecen **entre corchetes [ ]**, corresponden a notas aclaratorias sobre la institución educativa, adaptación y desarrollo de la sesión.

Los **textos normales**, corresponden a los mensajes clave e ideas a transmitir a los estudiantes.

Los **textos que se encuentran entre paréntesis ( )**, corresponden a aclaraciones o explicaciones ampliadas en cuestiones que pueden ser relevantes, por ejemplo, para responder a una pregunta.

La presentación incluye mensajes breves y directos, acompañados de imágenes decorativas/aclaratorias que captan la atención de los adolescentes, de modo que quien imparte la charla debe adecuarla al grupo haciendo y ampliando las explicaciones pertinentes.

Esta sesión se enfoca en la normalización de la actividad autónoma de los adolescentes en Internet y, por tanto, en el fomento de la responsabilidad que supone, para protegerse a sí mismos frente a los riesgos. El objetivo es que los preparemos con conocimientos y habilidades para que la prevención sea la clave de su seguridad en Internet. También el que les formemos estrategias para saber cómo actuar en caso de problemas.

Es importante que les tratemos como personas capaces de conocer e interiorizar información y conocimientos, son jóvenes que tienen capacidad para entender a qué nos referimos con riesgos. Prevemos hacerles más conscientes, recordarles información que posiblemente han oído anteriormente y reforzarla con nuevas recomendaciones. Es por ello imprescindible hacer una valoración al inicio de la sesión, en la que tanteemos la experiencia general del grupo y poder adaptar las explicaciones a esta premisa.

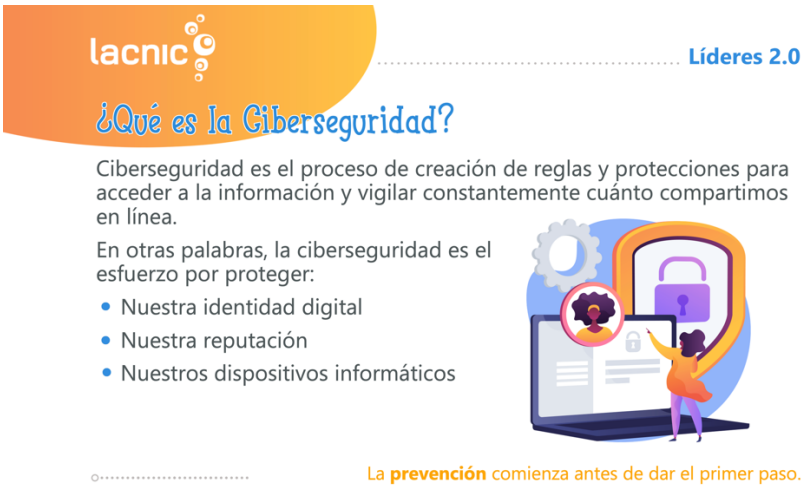
Queremos fomentar un uso creativo y reflexivo de la Internet e inculcar hábitos digitales positivos, promoviendo respeto, naturalidad y tolerancia.

Diapositiva 1. Inicio

[Antes de iniciar la sesión, prepara la presentación para mostrarla a pantalla completa con esta primera diapositiva].

Preséntate brevemente e introduce el tema y los objetivos de la sesión: muéstrales a los estudiantes cómo utilizar Internet de forma segura en su día a día, señálales algunos de los riesgos que pueden encontrarse y cómo afrontarlos.

Diapositiva 2. ¿Qué es la Ciberseguridad?

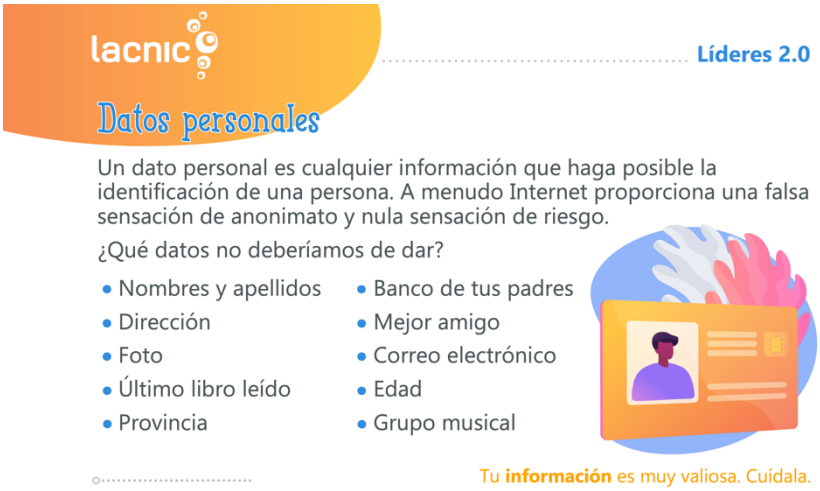


[A modo de introducción, indaga en el grupo para valorar el conocimiento que poseen en torno a Internet y a la Ciberseguridad. Procura partir de sus conocimientos para desarrollar el tema].

El objetivo es que el grupo comprenda la importancia de la seguridad en Internet y en sus dispositivos móviles:

- Aprender a apreciar el valor de nuestra intimidad y nuestros datos personales.
- Conocer pautas básicas de ciberseguridad.

Diapositiva 3 y 4. ¿Qué son los datos personales?



Los datos personales son aquellos que pueden servir para identificarnos en un contexto determinado. Hay que tener en cuenta que, quizás, un dato aislado en un determinado momento o contexto no es suficiente para identificar a una persona. Sin embargo, si existen otros datos en otros lugares de la Red y es posible relacionarlos entre sí, se puede llegar a identificar a la persona. En ese caso, nuestra privacidad puede verse comprometida si terceras personas usan esa información sin nuestro conocimiento con intenciones de gastarnos una broma, reírse un rato, obtener un beneficio, etc. Aunque todos los datos personales son importantes, quizás la imagen, nuestra fotografía, es el que nos identifica con mayor claridad.

El mensaje clave para los estudiantes de modo que cuiden su privacidad es que reflexionen siempre antes de compartir información personal, porque cuando navegan pueden llegar a dar más información de ellos de la que quieren dar y una vez publicada o compartida no podrán eliminarla de la Red: ¿puede suponer un riesgo compartir esta foto o este dato?, ¿qué pasaría si se hace pública y la ve todo el mundo?, ¿podrían utilizar esta información para hacerles daño?, ¿hay más personas implicadas cuya privacidad deben respetar?

(Pregunta al grupo ¿Qué datos no deberíamos dar?, y muestra el listado, espera para que ellos opinen y una vez hayan participado pasa a la siguiente diapositiva donde aparecerán tachados aquellos datos que NO debemos compartir en Internet).

[Anima a los estudiantes a reflexionar sobre la presión social que empiezan a sentir por unirse a las redes sociales y compartir todo lo que hacen en su día a día. También plantéales que no es necesario publicar información privada para ganarse el reconocimiento social].

Igualmente es importante que se percaten de que todo lo que hacen en Internet deja un rastro, una huella digital que habla de ellos. ¿Sabías que toda la información que dejas cuando te conectas forma lo que se llama tu identidad digital?

Diapositiva 5. Identidad Digital

[Conversa con el grupo sobre Internet como la fuente principal de información que en la actualidad se tiene para conocer a alguien. Ya sea por medio de un sitio o página web, o bien por redes sociales, brinda la posibilidad de acceder a información personal de quien se busque. Por eso es primordial el cuidado de lo que se sube, ya que Internet es la vidriera a través de la cual el mundo nos conoce].

La identidad digital se forma a partir de la información que sobre nosotros se sube a Internet, tanto por nosotros mismos como por amigos, compañeros o familiares.

Cada vez que hacemos clic en un "me gusta", subimos una foto o compartimos un video, no solo estamos expresándonos, también estamos contribuyendo a crear las tendencias que conforman la realidad de Internet. Todo ello tiene valor en sí mismo,

es relevante en la definición de nuestra personalidad y provoca consecuencias tanto positivas como negativas.

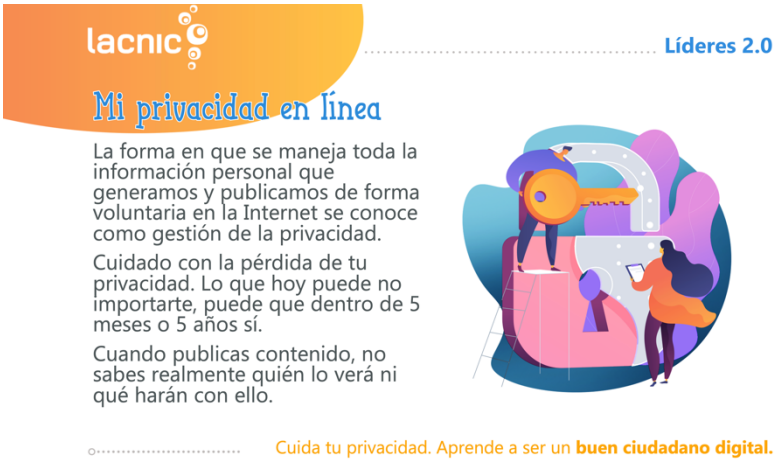
Diapositiva 6. ¿Cómo se construye nuestra identidad digital?

La huella digital incluye las publicaciones que un usuario realiza, aquellas en las que sea etiquetado o mencionado, las fotos o videos personales o subidos por otros, las páginas web donde se cite su nombre, las cuentas de usuario en redes sociales que estén asociadas a su nombre real, las noticias referidas a su persona, y la participación como usuario en foros, salas de juegos, de chat u otros.

La identidad digital es lo que somos para otros en la Red o, mejor dicho, lo que la Red dice que somos a los demás.

[La información de la identidad digital puede producir efectos positivos y negativos en el mundo real].

Diapositiva 7. Mi privacidad en línea



[Explica al grupo el concepto de privacidad, dado que para ellos este no es un riesgo tan evidente como otros. Para los adolescentes, la privacidad suele estar asociada a guardar en secreto frente a los adultos parte de su información más íntima, pero no dudan en compartirla con su grupo de iguales o incluso con desconocidos. No siempre son conscientes de las consecuencias de una mala gestión de la privacidad].

¿A qué nos referimos con privacidad? En Internet todos compartimos mucha información sobre nosotros mismos: escribimos comentarios y opiniones, publicamos fotos y videos, mostramos quienes son nuestros amigos y familiares, etc. Por ejemplo, cuando observamos la cuenta de Instagram de personas muy conocidas, las cuales suelen compartir miles de imágenes personales. ¿Son demasiadas? ¿Qué información están aportando con estas publicaciones? El cuidado de la privacidad depende de qué información deciden mostrar y en qué cantidad, y qué datos prefieren guardarse para sí mismos.

¿Cuánta información sobre ellos existe en Internet? Deben ser conscientes de que no solo comparten información en las redes sociales, también al enviar mensajes a sus contactos de WhatsApp por ejemplo, o al comunicarse con otros jugadores en un videojuego. Pero además otras personas publican datos sobre ellos, y algunos servicios de Internet también recogen información.

¿Pero por qué se considera un riesgo? El problema radica en que, una vez que comparten su información privada, pasa a ser pública y es un paso que no tiene marcha atrás. Más adelante pueden arrepentirse de haber compartido esos datos o esas imágenes, y estos pueden acabar en manos de personas desconocidas que pueden utilizarlos para hacerles daño.

(Explica al grupo el siguiente ejemplo: Ponte en esta situación cuando vayas a enviar una foto o subirla a tu red social. Imagina que coges una foto en papel tuya y vas a una tienda a que te impriman a tamaño poster 100 copias. Luego las vas pegando por diferentes lugares de la ciudad, en la entrada de tu colegio, en la plaza principal, en el súper, y los postes de la calle. Mucha gente la va a ver y puede que alguien la pintarrajee, fotografíe, o se la lleve a casa. Algo así supone subir una foto a Internet).

[Enlace de interés: https://www.is4k.es/necesitas-saber/privacidad]

Diapositiva 8. Redes Sociales

[Es posible que algunos estudiantes manifiesten que no tienen o no les permiten en casa tener redes sociales, y debes fomentar la normalización de esta situación: es una elección personal, deben contar con la autorización familiar y la recomendación ante todo es estar preparado antes de crearse un perfil].

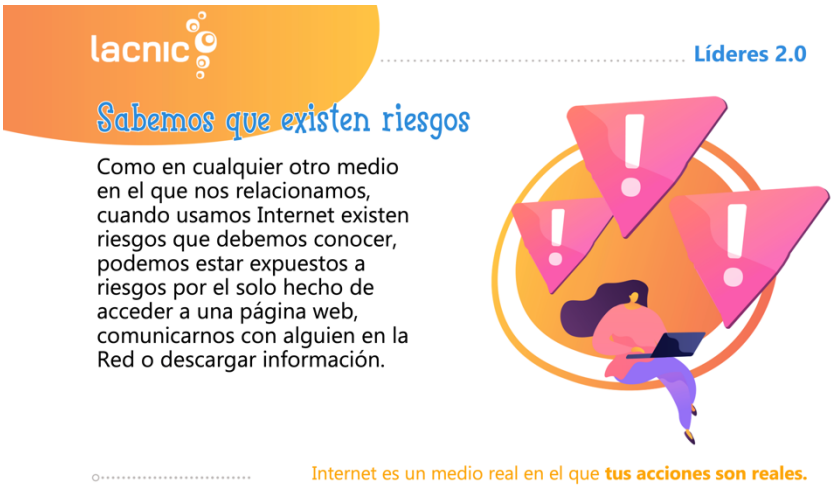
(En la imagen aparecen los logotipos de Tik Tok, Instagram, WhatsApp, Facebook, Pinterest, Snapchat, Twitter y YouTube).

Pregunta al grupo acerca de los logotipos que aparecen en pantalla, ¿los conocen? Seguramente sí, aunque aún no los utilicen todos, pero algunos sí serán habituales en su tiempo de ocio. ¿Cuánto tiempo dedican a utilizar las redes sociales?, ¿por qué les interesan?, ¿qué ofrecen las redes sociales? Comunicación, sentimiento de comunidad, entretenimiento, etc. En definitiva, son una herramienta que permite la relación con otras personas. Primero habla en este punto de funciones positivas, beneficios que hacen de las redes sociales un medio útil y atractivo. Por último,

plantea al grupo la posibilidad de que también existan riesgos en el uso de estos servicios, ¿los conocen?

[Deja que sean ellos mismos los que expongan sus ideas al respecto, de modo que puedas valorar su experiencia y conocimientos para adaptar las explicaciones posteriores].

Diapositiva 9. Sabemos que existen riesgos



Plantea al grupo la posibilidad de que existan riesgos en el uso de Internet. En lugar de limitarte a explicar riesgos y hacer un listado de cuidados a tener y situaciones a evitar, crea escenarios ficticios y anima a los estudiantes a comentar sobre ellos, es una buena forma de que se enteren sobre los peligros y entiendan mejor por qué y cómo deben protegerse. El objetivo es propiciar que lleguen a sus propias conclusiones y averigüen las respuestas por sí mismos. Estos escenarios son muy útiles para enseñar cómo manejar situaciones dolorosas, incómodas o peligrosas.

[Deja que sean ellos mismos los que se animen a comentar algunos problemas derivados de un mal uso de Internet, de esta manera podrás hacerte una idea de su experiencia con Internet y el uso que le dan].

Pregunta a los estudiantes, ¿quién podría aprovechar brechas de seguridad en Internet para ver información personal? (Las posibles respuestas incluyen hackers malintencionados, agentes de vigilancia del gobierno, etc.).

Explica que los hackers malintencionados, cuando exploran la web, pueden recopilar datos sobre ellos del mismo modo que lo hacen los proveedores de servicios de

Internet. Para reducir este riesgo, deben usar una conexión segura con el sitio o los sitios web a los que intentan acceder. Por otro lado, muchos sitios web buscan hacer un seguimiento de sus patrones de consumo en varias plataformas, independientemente de la conexión que usen. Pueden ver su navegador, ubicación y otros patrones de consumo para intentar averiguar quiénes son.

(Insiste en que los riesgos son una realidad, que cualquiera puede verse afectado y que para lograr el objetivo de un uso de Internet más seguro, deben tener claro que las mismas reglas que se aplican en el mundo offline/mundo real son las del mundo online/mundo digital).

Diapositiva 10. ¿Qué es un contenido inadecuado?

Internet ofrece un espacio inmenso en el que relacionarnos y obtener información de toda clase de temas, pero algunos de ellos son perjudiciales y pueden tener consecuencias graves.

Un contenido inapropiado es todo material percibido por el menor de edad que sea dañino para él. Son las imágenes y estímulos que provocan un perjuicio en el menor, aquellos peligros que circulan por la Red y las características de la información que contienen. Dentro de esta acepción, conviene distinguir entre contenidos ilícitos, que son aquellos que no están legalmente permitidos; y los contenidos nocivos, que sí están permitidos por Ley pero se consideran dañinos en el desarrollo personal y social de los menores.

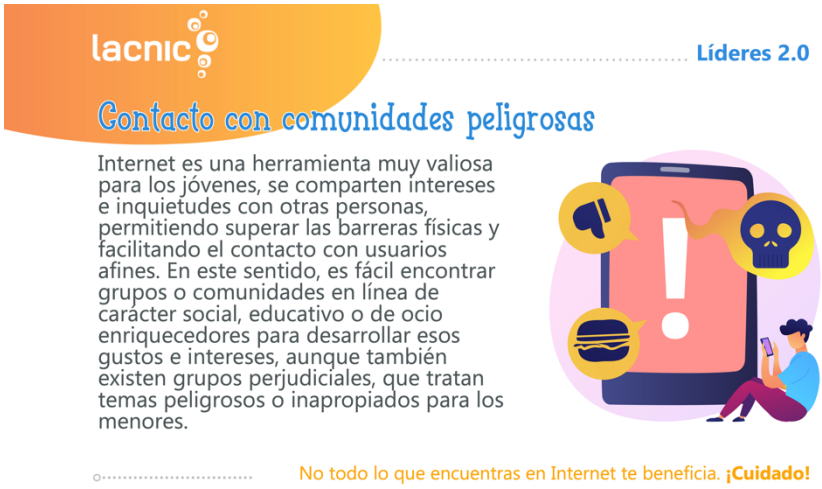
[Los principales tipos de contenidos inapropiados:

- La pornografía, información e imágenes sexuales explícitas con el fin de provocar la excitación del receptor.
- La violencia, empleo intencional de la fuerza o poder físico, de hecho o como amenaza, contra uno mismo u otro/s que pueda causar daños físicos o psicológicos, trastornos del desarrollo o privaciones (física, psicológica, sexual, patrimonial).
- Los contenidos falsos, informaciones erróneas o visiblemente falsas que circulan por Internet y llegan fácilmente a un gran número de receptores debido a la naturaleza del contenido y la tendencia a propagarse rápidamente (leyendas urbanas, mensajes en cadena, virales).
- El fomento del consumo de drogas, sustancias introducidas en el organismo que producen una alteración del natural funcionamiento del sistema nervioso central, crean dependencia física y/o psicológica, y provocar daños y enfermedades físicas graves.
- El fomento de acciones que dañan la salud física y psicológica (trastornos de la conducta alimentaria, cirugía estética, blanqueamiento dental etc.), consecuencia de los ideales de belleza y el aspecto corporal dominante, en función de cañones cultural, social y mediáticamente establecidos.
- Los juegos de azar y apuestas, donde la búsqueda de beneficio económico trae consigo el riesgo de ser engañado, o perder cantidades considerables de dinero.
- La afición a los videojuegos y juegos online, que puede convertirse en un riesgo grave cuando se convierte en adicción provocando aislamiento familiar y social, trastornos actitudinales, de personalidad y de conducta.
- La publicidad online, medio carente de filtros para que las empresas se publiciten, llegando fácilmente a un gran número de personas en todo el mundo.
- La Ingeniería social, práctica informática delictiva para conseguir información sensible, personal y confidencial, manipulando y engañando a los usuarios legítimos].

Una vez que los estudiantes conocen qué son los contenidos inapropiados y qué tipos pueden encontrar es conveniente analizar por qué acceden a estos contenidos. Haz al grupo dos preguntas abiertas para generar debate: ¿Qué motivaciones tienen ustedes para acceder a este tipo de contenido? ¿Qué riesgos puede suponer el acceso a contenidos inapropiados?

[Enlace de interés: https://www.is4k.es/necesitas-saber/contenido-inapropiado]

Diapositiva 11. Contacto con comunidades peligrosas



[Sondear si los estudiantes han estado en contacto con este tipo de comunidades y cuál es su experiencia. El docente lanzará preguntas abiertas al grupo del tipo: ¿Alguien conoce alguna comunidad peligrosa online?, ¿de qué tipo? ¿qué mensajes les transmiten?].

Hablamos de comunidades en las que, por ejemplo, se habla de hábitos poco saludables, o en las que se transmiten ideologías extremistas que fomentan el odio. En muchos casos, hay personas cuya función es captar usuarios que muestren cierto interés por estos temas en la Red, atacando sus inseguridades e inquietudes, para luego introducirles en una comunidad que será dañina y de las que no es fácil salir.

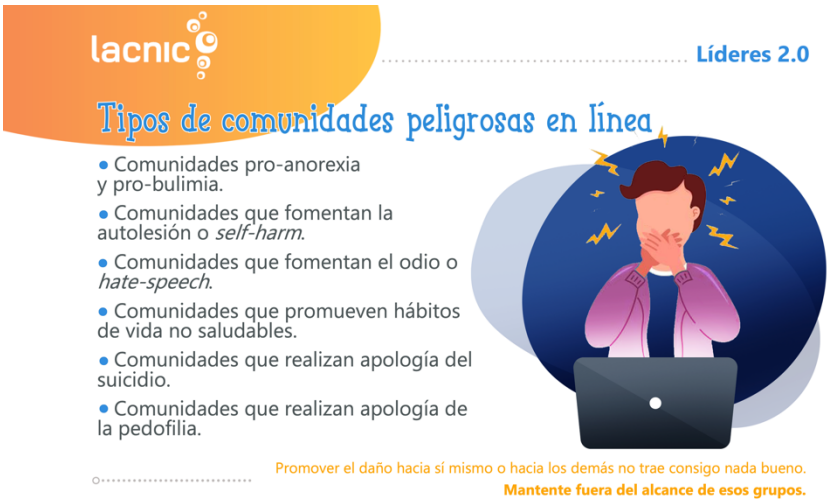
Diferencias entre comunidades en línea y comunidades peligrosas en línea:

Podemos definir las comunidades en línea como grupos de personas que carecen de un lugar físico, cuyas interacciones están marcadas por intereses comunes y que tienen una identidad dentro de un espacio en Internet. En función del interés común podemos encontrar diferentes tipos de comunidades, diferenciando por ejemplo: comunidades educativas, sociales, de ocio...

Las comunidades en línea no suponen un peligro por sí mismas, aunque sí se convierten en un riesgo en el momento en el que el contenido es inapropiado para los menores o se trata de comunidades peligrosas.

[Enlace de interés: https://www.is4k.es/necesitas-saber/comunidades-peligrosas]

Diapositiva 12. Tipos de comunidades peligrosas en línea



Los principales tipos de comunidades peligrosas que podemos encontrar en la Red son:

- Comunidades pro-anorexia y pro-bulimia: los miembros pro-ana son generalmente chicas jóvenes (aunque cada vez son más los casos de chicos) que sufren anorexia y que comparten sus ideas y sus consejos a través de páginas web, foros o blogs. Sus miembros apoyan la delgadez y la pérdida de peso extremas y dan consejos para conseguirlas.
- Comunidades que fomentan la autolesión, *self-harm*: entran en este grupo cualquier tipo de comunidad o grupo en Internet que promueva prácticas de autolesión, independientemente del objetivo de las mismas.
- Comunidades que fomentan el odio, *hate-speech*: se incluyen en esta clasificación los grupos o comunidades en línea que propagan, incitan, promueven o justifican el odio racial, la xenofobia, el antisemitismo, u otras formas de odio basadas en la intolerancia, incluida la intolerancia expresada por el agresivo nacionalismo y el etnocentrismo, la discriminación y la hostilidad contra las minorías, los inmigrantes y las personas de origen inmigrante. Así, esas comunidades fomentan a través de la Red, la discriminación de estos colectivos y la incitación a conductas violentas y perjudiciales contra ellos. Es lo que en la Red se conoce como «Ciberodio».

- Comunidades que promueven hábitos de vida no saludables: se incluyen en este grupo todas aquellas comunidades que incitan a los jóvenes al consumo de alcohol y drogas, entre otros malos hábitos.
- Comunidades que realizan apología del suicidio: en este grupo se incluyen aquellos sitios web que ofrecen información sobre los diferentes procedimientos para llevar a cabo un suicidio, incitando del mismo modo a su realización.
- Comunidades que realizan apología de la pedofilia: estas comunidades en la web no suelen contener imágenes de abusos o pornografía infantil explicita. Por el contrario, su funcionamiento y razón de ser se orientan a realizar una defensa de las relaciones entre adultos y menores, normalizando el delito implícito en ellas y buscando tanto seguidores como víctimas.
- Comunidades relacionadas con juegos online: no podemos dejar de lado el riesgo que supone entrar en contacto con comunidades peligrosas que promuevan la propia adicción a este tipo de juegos y la relación con colectivos y temáticas incitadoras de violencia, discriminación o actitudes inadecuadas.

[Evita alimentar en exceso su curiosidad por estos temas, dado que pueden llamar su atención de forma contraproducente, y que luego quieran buscar más información. Por ello enfócate en las consecuencias negativas y las estrategias de captación, no mencionando nombres de comunidades o hashtag concretos por ejemplo, y en ningún caso contenidos determinados, como videos o páginas web].

Diapositiva 13. Decimos NO al Ciberacoso

[Recuérdale al grupo el concepto de ciberacoso y sus características].

En este apartado intenta dar a los estudiantes la noción de **respeto y convivencia** en la Red. La convivencia digital no se distingue de la convivencia de la vida real y los adolecentes deben ser conscientes de que sus palabras o sus hechos pueden ofender o dañar a otras personas y que en ningún caso en la Red se debe de hacer algo que no se haría en la vida real.

El ciberacoso se manifiesta como un daño intencional y repetido a través de Internet y los diferentes medios en los que este se utiliza. Es una problemática muy normalizada en la actualidad, tanto que en muchos casos ni siquiera se considera acoso desde el punto de vista de los menores e incluso de los adultos. Pero el ciberacoso no es una broma y puede darse en diversas plataformas y formatos, como publicaciones, memes, videos, hashtags, exclusiones en grupos de WhatsApp, comentarios, etc.

[Enlace de interés: https://www.is4k.es/necesitas-saber/ciberacoso-escolar]

Diapositiva 14 y 15. Formas de Ciberacoso

¿Por qué lo hacemos? Las motivaciones para mantener este tipo de prácticas tan dañinas son diversas, desde la presión de los compañeros y la búsqueda de popularidad, hasta deseos de venganza o por falta de autoestima. Debes recalcar al grupo que en ningún caso está justificado herir de esta forma a un compañero.

[La falsa sensación de anonimato, de la mano de la soledad en la que suele establecerse la conexión, permite que quienes no se animan a discriminar en forma presencial, tengan más facilidades para hacerlo vía web, ya sea compartiendo

imágenes, con un "me gusta" a cierta publicación o comentando publicaciones discriminatorias que entran en el escenario del hostigamiento online].

¿Qué pueden hacer? Existen muchas formas de actuar frente al ciberacoso, empezando por no difundir y frenar la cadena de divulgación del mismo. Cada 'me gusta' o cada vez que se comparte un mensaje humillante cuenta, del mismo modo que si se participa en grupos creados para ofender y burlarse de una persona.

El apoyo a la víctima puede marcar la diferencia, ¿les gustaría sentirse solos ante esta situación? Ante la excusa habitual de «si me pongo de su parte me acabaran atacando a mí», la respuesta es que si todos mostrásemos nuestro rechazo, los acosadores no se sentirían capaces de atacar. Y recordemos que cualquiera puede ser víctima de ciberacoso, y en ese caso, también necesitaremos apoyo.

A modo de cierre de este tema, enfatiza en la importancia de crear un ambiente positivo en Internet. Procurar crear conciencia sobre una adecuada convivencia digital que redunde en lo que podríamos denominar *salud digital.*

Diapositiva 16 y 17. Grooming ¿Qué es?

[Describe brevemente el concepto de grooming y las claves para identificarlo].

Pregunta y explícale al grupo: ¿saben que es el grooming? Es una realidad que hay personas tienen malas intenciones y utilizan Internet como medio para que se acerquen a ellos. Recordemos que cualquiera puede crear un perfil falso, cambiar su imagen, su edad y aparentar tener gustos parecidos a los suyos. De esa forma, se

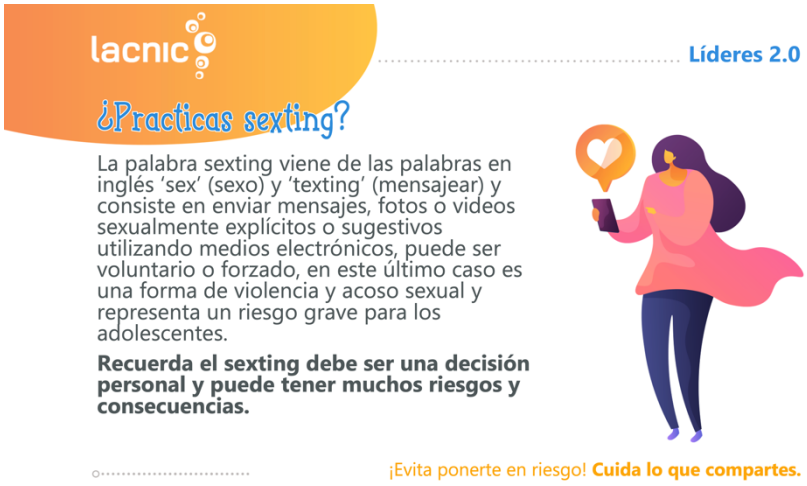
ganan su confianza, consiguen que acepten su solicitud de amistad y comienzan a conversar con ustedes.

Cuando ya tengan una relación afianzada, les pedirán una imagen o un video de connotación sexual, y habrán logrado su objetivo. A partir de ahí pueden chantajearles para conseguir más contenidos de este tipo, dinero o incluso que queden a verse en persona, todo con la amenaza de que si no lo hacen difundirán lo que ya está en su poder. Estas personas utilizan todas las plataformas y redes sociales que ellos utilizan, porque saben que ahí encontrarán jóvenes y que es un lugar donde se puede establecer una comunicación.

[Enlace de interés: https://www.is4k.es/necesitas-saber/grooming]

(Enlace a un video: https://www.youtube.com/watch?v=_whpii1co1g)

Diapositiva 18. ¿Practicas sexting?



[Dado que es un tema delicado e íntimo, procuraremos no hacer preguntas a participantes concretos. Se trata de mantener un tono cercano pero serio, para que comprendan que en ningún caso es una práctica sin riesgos].

Hacerse fotos o grabarse videos con cierta connotación sexual puede parecer divertido o tentador, pero lo cierto es que supone muchos riesgos. Por mucho cuidado que tengan, el simple hecho de almacenar ese tipo de imágenes en el teléfono celular o en el computador es muy arriesgado. Pueden perderlo, que se lo roben, o que sea infectado por un virus informático, por ejemplo. Son situaciones

que ocurren a diario. ¿Han oído noticias sobre famosos que han pasado por algo así? Es bastante habitual hoy en día y le puede pasar a cualquiera.

Si además de crear esa foto o video, la envían, el riesgo se multiplica. Están poniendo en manos de otra persona su privacidad. Y, a pesar de que en ese momento confíen plenamente en la otra persona, las cosas pueden cambiar o no ser tan seguras como pensamos. ¿Les suena eso de «te la paso pero no se la ensenes a nadie»? La difusión en estos casos es imparable.

Y recordemos que, si antes corrían riesgo por guardar esas imágenes en su teléfono celular, ahora el riesgo se multiplica de nuevo: son como mínimo dos teléfonos celulares los que almacenan ese contenido y que pueden perderse o ser robados. El riesgo es muy alto.

Por ello, la recomendación es no realizar esta práctica, ni tampoco pedir a otras personas que la practiquen. Es una forma de respetar y respetarse, de cuidar nuestra intimidad: se trata de protegernos y proteger a la otra persona de las consecuencias. Además, hay que tener en mente que el simple hecho de tener imágenes íntimas de otros menores en el teléfono celular puede considerarse un delito, más aún si se difunden. No es un juego.

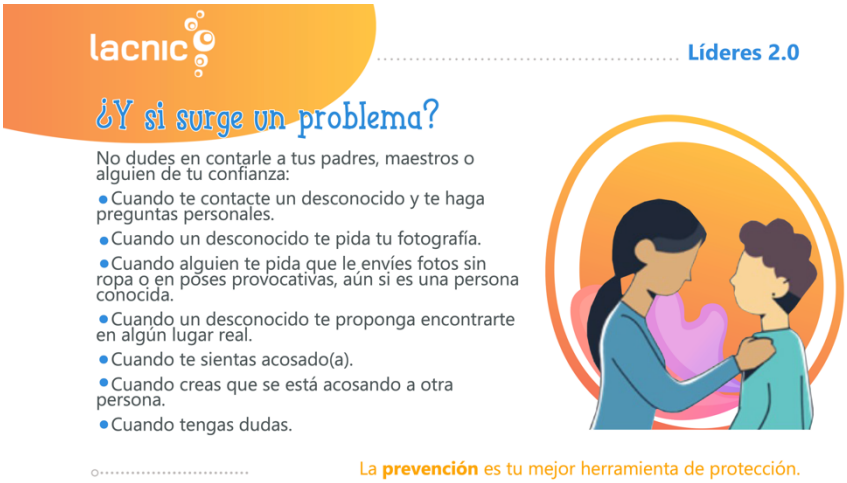
[Enlace de interés: https://www.is4k.es/necesitas-saber/sexting]

Diapositiva 19. El WiFi gratis te puede salir caro

[Los menores utilizan habitualmente estas redes públicas en cafeterías o centros comerciales, sin percatarse de que puede suponer un riesgo].

Es importante extremar la precaución al usar este tipo de redes públicas. Cualquiera podría ver qué páginas web visitan o qué hacen en ellas cuando usan esas redes, de modo que no deben emplearlas para entrar en sus redes sociales (con usuario y contraseña) o realizar compras, por ejemplo. Lo mismo sucede con las apps que no cifran la información que se envía y recibe (para comprobarlo se puede buscar información en el centro de seguridad o la ayuda de la app).

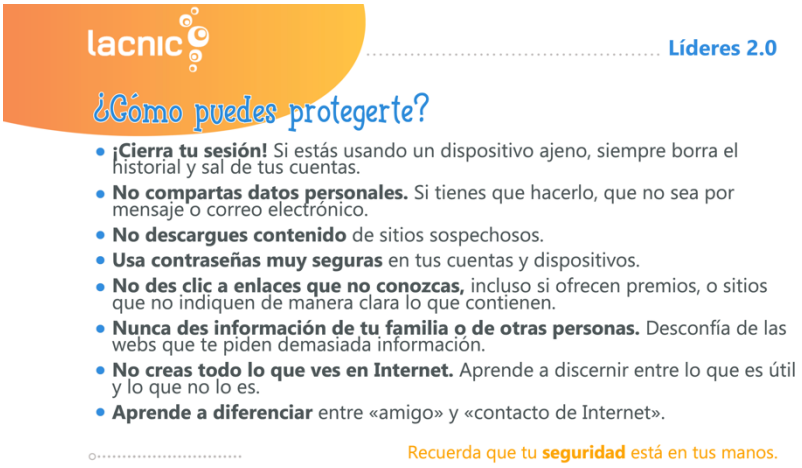
Diapositiva 20. ¿Y si surge un problema?



[Es esencial que les des la certeza a los estudiantes de que siempre existe una solución para cualquier problema que surja en Internet. Aunque resulte evidente que ante una situación compleja un estudiante puede no saber cómo actuar o pedir ayuda].

Es cierto que no se puede volver atrás, y puede que haya consecuencias, pero se puede salir adelante de cualquier situación siempre que contemos con el apoyo de un adulto de confianza y profesionales especializados. Por ello, les recordaremos que pedir ayuda es sencillo. Con la ayuda de un adulto, encontraran la manera de solucionar paso a paso el problema. En un principio puede parecer que es una situación imposible de arreglar, pero poco a poco verán que se puede salir adelante y afrontar las consecuencias.

Diapositiva 21. ¿Cómo puedes protegerte?



[A pesar de utilizar habitualmente teléfonos celulares, tabletas y computadores, los estudiantes no siempre conocen pautas básicas de seguridad para hacer un buen uso de los mismos. A modo de introducción en la ciberseguridad técnica, explícales cómo hacer una correcta gestión de acceso].

(Como adultos, debemos estar preparados para ayudar a los adolescentes a resolver los problemas, situaciones o preguntas que pudieran tener relacionadas con sus interacciones en línea. Es importante conocer cómo se comportan e interactúan, qué contenido buscan, las principales actividades que realizan y las tendencias actuales del mundo digital; entre más información y conocimiento tengamos a nuestro alcance, podremos reaccionar mejor y proporcionar consejos y/o soluciones).

¿Qué problemas nos podemos encontrar mientras navegamos por la Red? Algunos riesgos como virus, fraudes, phishing (páginas web que parecen ser auténticas pero que en realidad no lo son, y que pueden utilizarse para recabar información del usuario fácilmente, como datos de acceso, contraseñas, etc.) u otras estrategias de ingeniería social, entre otros.

Para protegernos, debemos tomar algunas medidas en nuestros dispositivos, son sencillas y seguro que las conocemos, pero ¿nos las tomamos en serio? Es necesario instalar un antivirus y mantenerlo actualizado, así como actualizar todas las aplicaciones que utilicemos y los sistemas de nuestro dispositivo. También debemos realizar copias de seguridad de nuestros datos periódicamente, procurar acceder a páginas web con certificado de seguridad (https) y descargar aplicaciones solo de desarrolladores oficiales.

Diapositiva 22. En Internet se puede

[Ten presente y házselo saber a los estudiantes que ser adolescente nunca ha sido fácil, porque a los retos de la edad se suma el escrutinio constante, por parte de los adultos, sobre lo bien o mal que hacen todo].

Los adolescentes usan la tecnología para jugar, entretenerse, hacerse series, experimentar, relacionarse. A veces corren riegos y a veces se equivocan. Pero a veces también crean, inventan, comparten y aportan, en positivo. A veces, sobre todo si se les anima, hacen mucho, mucho más. Internet es un gran recurso en muchos sentidos, solo hay que saber aprovecharlo.

Diapositiva 23. Fin

Sugerencias didácticas

Complementa la sesión con otras actividades para asimilar lo aprendido: ¡te proponemos algunas ideas!

Organiza debates en el aula sobre los siguientes temas:

- el ciberacoso escolar: «¿somos conscientes del daño que provoca el ciberacoso?»
- sobre el derecho al olvido: «¿qué hay de la información que se publica y que es difícil de borrar?»
- la privacidad en la Red: «¿todo vale con tal de conseguir más 'Me gusta' en Internet?»
- nuestros contactos en Internet: «ventajas e inconvenientes de tener muchos contactos en las redes sociales»
- la práctica del sexting y sus riesgos: «¿existe presión social para que los jóvenes practiquen sexting?»

Crea por grupos un mural digital en el que los estudiantes ilustren de forma creativa los consejos para:

- actuar frente al ciberacoso entre compañeros
- pensar antes de publicar o compartir cierta información
- evitar perder nuestra privacidad en Internet
- los consejos para elegir bien a nuestros contactos en Internet
- los consejos para evitar que nadie nos chantajee en Internet

Anima a investigar en Internet:

- cuáles son los motivos que mueven a los jóvenes a acosar a un compañero/a, y preparar por grupos una reflexión sobre ello para compartirla en clase.
- cuál es la relevancia de utilizar los mecanismos técnicos que las redes sociales ofrecen para publicar información, restringiendo el público que puede acceder a ellas.
- cuáles son las opciones de privacidad en las redes sociales más utilizadas y elaborar por grupos fichas prácticas sobre cómo configurarlas adecuadamente.

- a qué riesgos nos enfrentamos al aceptar solicitudes de amistad de desconocidos.
- qué es la extorsión y buscar recursos en línea para trabajar esta temática.

Sugiere buscar noticias en periódicos de Internet sobre:

- casos reales de chicos y chicas que han sufrido las consecuencias del ciberacoso.
- casos reales de chicos y chicas que han visto expuestos al ser asociados con información que tiene sentido en un ámbito privado pero otro diferente en el público
- casos reales de chicos y chicas que han tenido problemas por perder su privacidad
- casos reales de chicos y chicas que han tenido problemas a causa de sus amistades en las redes sociales
- casos reales de chicos y chicas que han sufrido chantajes en Internet

Otro recurso para tus estudiantes es la Biblioteca de cultura digital que ofrece planes de estudio diseñados por expertos para ayudar a los jóvenes a desarrollar las competencias necesarias para transitar el mundo digital, consumir información de forma crítica, y producir y compartir contenido de manera responsable, al cual puedes accesar en el siguiente enlace:

- https://www.facebook.com/safety/educators

COLABORADORES
del proyecto

Noralí Duin Picón
Ingeniero de Sistemas - MSc en Gerencial Empresarial
Directora del Comité de Educación de ISOC Panamá
Coordinadora General del Proyecto y desarrollo de contenidos

José Antonio Maldonado
Consultor en estrategia y marketing digital
Conceptos estratégicos y desarrollo de contenidos

Eysabel Méndez
Licenciada en Educación - Magister en Gerencia Tecnológica
Máster Internacional en enseñanza y aprendizaje abierto y a distancia
Especialista en Diseño Instruccional y Contenido
Validadora de los Instrumentos

Gustavo Polanco
Licenciado en Artes, mención Diseño Gráfico
Artista plástico e Ilustrador

Dilia Tallaferro
Licenciada en Educación, mención Preescolar
Diploma de estudios avanzados (DEA) en Didáctica y organización escolar
Correctora de Estilo

Alex Barrios
Desarrollador Fullstack y certificado experto en seguridad informática
Validador de los Instrumentos

Juan Moreno
Licenciado en Química - Licenciado en Educación
mención ciencias naturales Matemática y Tecnología
MSc en Tecnología Educativa
Validador de los Instrumentos

Naive Ángulo
Licenciada en Estadística
Analista de Datos (Instrumentos)

Daniel Alejandro Chacin
Asistente General

Nigel Cassimire
Especialista en Telecomunicaciones
Mentor de LACNIC

REFERENCIAS Documentales

- Agencia Española de Protección de Datos (s.f.) España: AEPD. Recuperado de **https://www.aepd.es/es**
- Ayuntamiento de Burgos (s.f.) *Guía tecnología e infancia*. España. Recuperado **http://www.aytoburgos.es/archivos/servicios-sociales/articulo/documentos/guia-tecnologia-e-infancia.pdf**
- Biblioteca de cultura digital (2021) *Módulos*. Facebook. Recuperado de **https://www.facebook.com/safety/educators**
- Freepik (2010-2021) *Galería de imágenes*. España: Freepik Company. Recuperado de **https://www.freepik.es/**
- Fundación para la Convivencia Digital (2021) Chile. Recuperado de **https://convivenciadigital.cl/**
- Internet Segura Is 4k For Kids (s.f.) *Presentaciones por edades*. España. Recuperado de **https://www.is4k.es/presentaciones-por-edades**
- Internet Segura Is 4k For Kids (s.f.) *Catálogos de Recursos*. España. Recuperado de **https://www.is4k.es/de-utilidad/recursos/recursos-didacticos-redes**
- Instituto Nacional de Ciberseguridad (s.f.) España. Recuperado de **https://www.incibe.es/**
- Observatorio de la Infancia en Andalucía (s.f.) España. Recuperado de **https://www.observatoriodelainfancia.es/oia/esp/index.aspx**
- Observatorio de la Infancia en Andalucía (s.f.) *Guía de tecnología e infancia*. España. Recuperado **https://www.observatoriodelainfancia.es/ficherosoia/documentos/7210_d_guia-tecnologia-e-infancia.pdf**
- Oficina de Seguridad del Internauta (s.f.) España. Recuperado de **https://www.osi.es/es**
- Pantallas Amigas (2004-2020) España. Recuperado de **https://www.pantallasamigas.net/**

REFERENCIAS Documentales

- Perle, L. (2021) *Principios fundamentales*. Facebook. Recuperado de **https://www.facebook.com/safety/youth/peer-voices/principles?locale=es_LA**
- Somos más contra el odio y radicalismo (s.f.) España. Recuperado de **https://www.somos-mas.es**
- Somos más contra el odio y radicalismo (s.f.) *Uso seguro*. España. Recuperado de **https://www.somos-mas.es/wp-content/uploads/2020/02/2-uso_seguro.pdf**
- UNICEF y Faro Digital (2020) *Guías de sensibilización sobre convivencia digital.* Recuperado de **https://www.unicef.org/argentina/informes/guia-de-sensibilizacion-sobre-convivencia-digital**