DEFENSORES DIGITALES

GUÍA DE ACTUACIÓN EN CIBERSEGURIDAD PARA DOCENTES E INSTITUCIONES EDUCATIVAS

H. AYUNTAMIENTO DE SAN LUIS POTOSÍ 2024-2027

San Luis amable

sanluis.gob.mx

@slpmunicipio

Índice

- **Los derechos digitales.**
- **Ciberseguridad otro concepto fundamental.**
- **Herramienta digital, ¿Verificación que?...**
- **¿Conoces los riesgos en línea que pueden afectar a tus estudiantes?**
- **Una tipología de los riesgos en línea a los que se enfrentan NNA.**

Capítulo 2/ Hablemos de delitos informáticos identifícalos para prevenir.

- **¿Qué tanto conozco sobre los delitos informáticos?**
  - Conoce las respuestas.
- **Conozcamos sobre delitos informáticos.**
- **¿Los Identificas?, te presentamos los delitos informáticos más comunes que vulneran a las NNA.**
  - Ciberbullying.
    - » Herramienta Digital.
  - Grooming.
  - Secuestro virtual.
  - Sexting.
  - Sextorsión.
    - » Herramienta Digital.
  - Happy slapping.
  - Phishing.
    - » Herramienta Digital.
  - Violencia online en la pareja o ex pareja.
  - Otras situaciones que pueden resultar riesgosas y que se deben considerar.
- **¿Tus estudiantes frecuentan estas páginas? Mantente alerta.**
  - Páginas gore y de narcocultura.
  - Páginas de flaming y comunidades tóxicas.
  - Plataformas +18 como OnlyFans.
  - Plataformas sociales como Reddit, 4chan o discord.
  - Navegadores de internet como Tor Browser, I2P, Whonix-Workstation.
  - DeepNude.
  - Páginas de compra y ventafraudes en compra por internet.
- **Actuación docente.**
- **Comunicación con Niñas, Niños y Adolescentes en riesgo.**
- **Comunicación con Niñas, Niños y Adolescentes con conductas antisociales en el mundo digital.**
- **Comunicación con madres, padres y cuidadores.**
- **Recomendaciones para hablar con cualquier tipo de madre, padre o cuidador.**
- **Conoce a tus aliados.**
  - ¿En dónde puedo contactarlos?
- **¿Cómo se lleva a cabo el proceso de denuncia?**
- **Aprende a guardar las pruebas.**

Capítulo 3/ Tecnología, tu gran aliada. Algunas aplicaciones y consejos que te ayudarán.

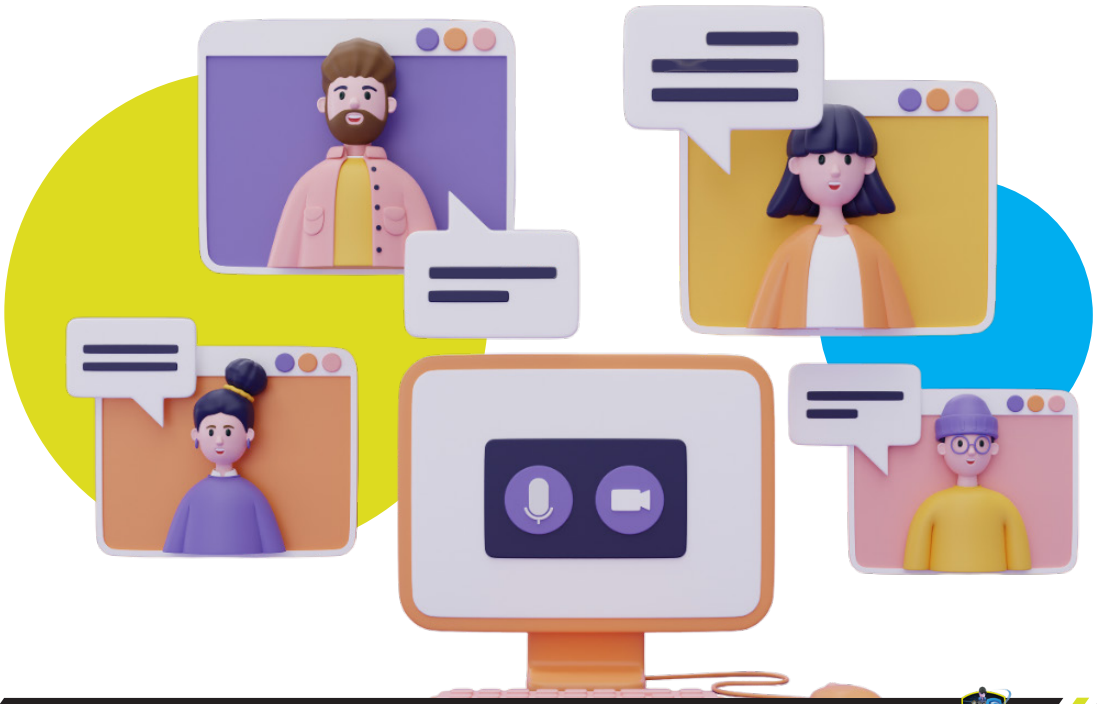
- **¿Por qué es importante la ciberseguridad en mi escuela?**
  - Conoce las respuestas.
- **SafeSearch o Búsqueda Segura de Google.**
  - Google Workspace for Education.
- **¿Tus estudiantes usan redes sociales?, conoce sus políticas de uso.**
  - Facebook.
  - Instagram.
  - X.
- **Vincula para prevenir ejemplos de cómo usar las redes sociales para la educación.**
- **Grupos de WhatsApp, una herramienta para el docente digital.**
- **Reglas para el buen uso del grupo de WhatsApp de madres, padres y cuidadores.**
- **Resolución de conflictos.**
- **Instituciones Amigas, ¿dónde puedes pedir ayuda?**
- **Glosario de términos.**
- **Referencias.**

Presentación de la Política Pública Defensores Digitales

El Gobierno Municipal 2021-2024 enfoca, prioriza y gestiona Políticas Públicas innovadoras buscando beneficiar a la ciudadanía. Comprendemos que la única manera de conseguir la ciudad segura que las y los potosinos merecen, es a través de la cooperación y coordinación de todos sus habitantes.

Desde el inicio de la administración, una de las estrategias principales de la Capital del Sí es el del desarrollo de estrategias y mecanismos en torno a la protección y fomento del sano desarrollo de niñas, niños y adolescentes (NNA), apoyados en herramientas novedosas de las que somos pioneros, partiendo de Derechos Fundamentales que señalan el derecho a vivir en un medio ambiente sano, sustentable, en condiciones que permitan un sano desarrollo, bienestar, crecimiento saludable, en que se desarrollan las estrategias que buscan favorecer a la ciudadanía, tal y como ocurre con este Compendio de actuación en ciberseguridad.

El Compendio de actuación en ciberseguridad para docentes e Instituciones educativas, nace de la prioridad de brindar información buscando la seguridad de niñas, niños y adolescentes, no solo en su entorno físico, sino también dentro de los medios digitales a los que se han visto expuestos durante la última década, es importante para nosotros proveer de un sentido de Seguridad digital para gestionar de manera informada la actividad en línea, así como guiar a los principales nucleos de desarrollo de NNA proporcionando información acerca de temas digitales de los que debemos estar atentos.

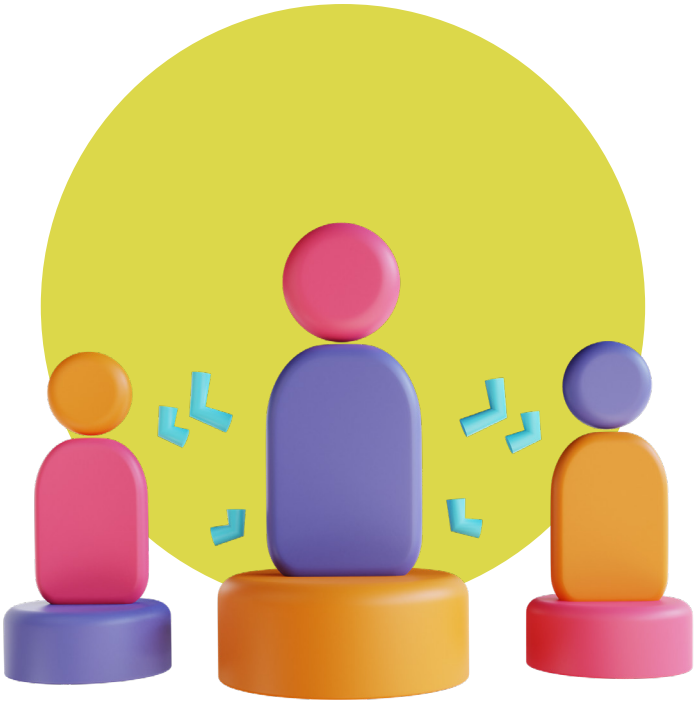


¿Cómo construimos la Política Pública?

El Gobierno Municipal 2021-2024, trabaja en coordinación con la ciudadanía, con prioridades claras, bajo el compromiso de crear estrategias cooperativas enfocadas en la seguridad y el desarrollo saludable y libre de violencia de niñas, niños y adolescentes, dentro y fuera del mundo digital.

Para procurar una ciudad segura a nivel digital será necesario contar con valores como la eficiencia, respeto, objetividad, profesionalismo, altruismo, colaboración y solidaridad, valores que se encuentran reflejados en el desarrollo y ejecución de la Política Pública.

La planeación de las acciones que se llevan a cabo dentro de esta Política Pública, se rige por medio de tres ejes estratégicos, así como tres líneas de acción correspondiente a cada eje, todo con respeto, promoción, y protección de los derechos de niñas, niños y adolescentes.



MISIÓN

El Gobierno Municipal 2021-2024, trabaja de manera coordinada con la ciudadanía, bajo el compromiso de crear estrategias cooperativas enfocadas en la seguridad y el desarrollo saludable y libre de violencia de niñas, niños y adolescentes, dentro y fuera del mundo digital, mediante procesos eficientes de prevención.

VISIÓN

Ser una ciudad cibersegura, con menos brechas digitales generacionales y con un sentido de autocuidado digital.

Ejes estratégicos

Sentido de ciberseguridad:

Una ciudad con un sentido positivo sobre el uso de las tecnologías de la información y comunicación.

Participación homogénea:

Participación por igual por y para los Potosinos en pro de niñas, niños y adolescentes.

Sentido de autocuidado:

Generar un sentido de autocuidado en el uso de las TIC por parte de la ciudadanía.

Líneas de acción

Formación:

Permite desarrollar capacidades que contribuyen a la transformación cultural para el mundo digital.

Fortalecimiento organizacional:

Contribuye a que las organizaciones tengan las herramientas necesarias para cumplir con sus compromisos y aseguren su continuidad y crecimiento.

Comunicación:

Es un instrumento fundamental para la movilización social, la visibilización de procesos, la sensibilización y difusión de temas centrales para el mundo digital.

Mensaje Del Presidente Municipal de San Luis Potosí

Tenemos un fuerte compromiso con la seguridad, el desarrollo y el futuro de nuestras niñas, niños y adolescentes, la política pública Defensores Digitales representa una respuesta innovadora y necesaria frente a los retos que plantea el entorno digital, reafirmando nuestro deber de proteger a quienes más lo necesitan.

Vivimos en un mundo donde la tecnología no solo transforma nuestra manera de comunicarnos y aprender, sino que también plantea riesgos reales, por ello, Defensores Digitales se erige como una propuesta visionaria que no solo protege, sino que también empodera.

Es una política pública que reconoce el valor de la prevención, la educación y la colaboración, marcando un nuevo estándar en la forma en que abordamos los desafíos de esta era tecnológica.

El éxito de esta política depende de la voluntad y el compromiso colectivo. Por eso, invito a todos los sectores de la sociedad a sumarse a este esfuerzo, porque cada acción cuenta, cada idea suma y cada paso nos acerca a garantizar que nuestras niñas, niños y adolescentes estén seguros y preparados para el mundo digital.

Este es un proyecto que habla de esperanza, de responsabilidad compartida y de la firme decisión de construir un mejor futuro, hagamos de Defensores Digitales un ejemplo de lo que podemos lograr cuando trabajamos juntos por el bienestar de nuestras niñas, niños y adolescentes.

Mtro. Enrique Francisco Galindo Ceballos
Presidente Constitucional
del Municipio de San Luis Potosí

Mensaje del Secretario de Seguridad Y Protección Ciudadana del Municipio de San Luis Potosí

Mi compromiso con San Luis Potosí, se amplía a proyectar la seguridad más allá del entorno físico, ya que la oportunidad de crecimiento tecnológico ha proporcionado nuevos medios para vulnerar a otros. Durante esta administración se busca proteger y apoyar a quienes se encuentren más vulnerables, y frente a la ciberdelincuencia está claro que los más propensos a los riesgos es nuestra ciudadanía más pequeña.

El nuevo reto es construir espacios ciberseguros para niñas, niños y adolescentes y la comunidad en general, que sepan que es posible construir entornos seguros en todos los ámbitos, haciendo frente a las nuevas tecnologías y cambios sociales que se presenten en torno a ellas, considerando los procesos de cambio frente a las formas de acceder a la información, la distancia entre el hacer tradicional y el hacer tecnológico y las nuevas oportunidades para la criminalidad.

Comisario. Mtro. Juan Antonio de Jesús Villa Gutiérrez
Secretario de Seguridad y Protección Ciudadana

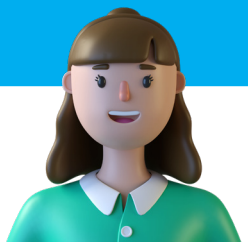
Antecedentes

De acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022, elaborada por el Instituto Nacional de Estadística y Geografía (INEGI), en el Estado de San Luis Potosí se identifico que:

Al 2022 en San Luis Potosí el

75.1%

de su población es usuaria de internet



A nivel nacional

93,052,870

personas son **usuarias de internet**

78.6%

son usuarios de internet de 6 años de edad o más representando **93.1 millones de personas** de la población nacional. (ENDUTIH, 2022)

3.9% de la población de 6 a 11 años de edad de San Luis Potosí es usuaria de un teléfono celular, mientras que el 13.2% es población de 12 a 17 años de edad.

FUENTE: Instituto Nacional De Estadística Y Geografía. (2022). Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022. https://www.inegi.org.mx/programas/dutih/2022/#informacion_general https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf

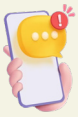
La digitalización en los procesos educativos.

VII ESTUDIO GLOBAL Sobre el uso de la tecnología en la educación, informe de resultados México 2022.

82%

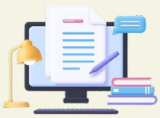
de los centros educativos en México han integrado la tecnología en el aula de algún modo, de estos, el **30% lo implemento a partir de la pandemia.**

Los **celulares** y las **computadoras** son los **dispositivos más utilizados dentro del aula por los estudiantes.**



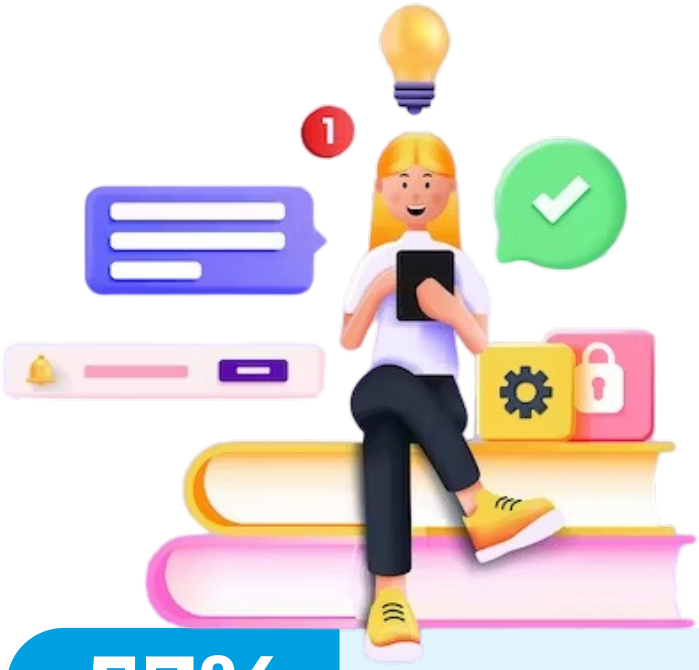
35%

DISPOSITIVOS MÓVILES



29%

COMPUTADORAS



Mayores retos durante el uso de tecnología en el aula

VII ESTUDIO GLOBAL Sobre el uso de la tecnología en la educación, informe de resultados México 2022.

57%	Problemas de conectividad.
47%	Dificultad para que el alumnado use las TIC más allá de fines recreativos.
36%	Escasa formación del profesorado en competencias digitales.
34%	Carencia de dispositivos para los estudiantes y docentes.
20%	Garantizar la seguridad y protección de datos de las NNA.

Los docentes demandan formación en competencias digitales

En 2022 sólo el 20% de los docentes recibieron formación por parte de su centro educativo según el VII Estudio Global sobre el uso de la tecnología en la educación (BlinkLearning, 2022).

FUENTE: BlinkLearning. (2022). VII Estudio Global sobre el uso de la tecnología en la educación. Informe de resultados México 2022.
file:///C:/Users/andreaojeda/Downloads/BLINK_VII_Estudio-TIC_Mexico_2022_469457[1].pdf

1 DOCENTES 2.0

Defensores Digitales

Compendio de actuación en ciberseguridad para docentes e instituciones educativas

En la Secretaría de Seguridad y Protección Ciudadana del Municipio de San Luis Potosí, sabemos que los temas digitales pueden parecer abrumadores, este **Compendio de actuación en ciberseguridad,** lo hemos desarrollado en colaboración con **profesionales en ciberseguridad y criminología** pertenecientes a la Dirección General de Tecnologías e Inteligencia Social de esta Secretaría de Seguridad y Protección Ciudadana del municipio de San Luis Potosí, buscando promover el sano y responsable desarrollo de NNA, además de promover el conocimiento acerca del mundo digital.

Consultar este Compendio puede ayudarte a ti como docente a comenzar un diálogo continuo con tus alumnas y alumnos sobre la seguridad dentro del mundo digital, conocer los riesgos a los que pueden ser expuestos, reforzar el sentido de ciudadanía digital de NNA y así, ser consientes de la seguridad en Internet, ademas de brindarte información sobre temas digitales que pueden serte de utilidad para tu carrera docente y la implementación de la tecnología en la educación.

Los invitamos a que se adentren a este Compendio y conozcan sobre ciberseguridad.

¿Eres un docente 2.0?
¡DESCÚBRELO!

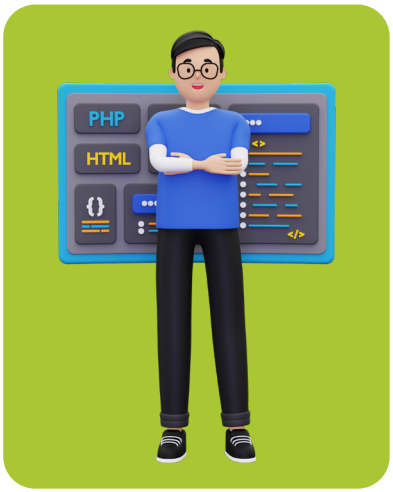
El uso y dominio de las TIC es una habilidad indispensable para el docente, integrarlas en el desarrollo de tus lecciones puede darte grandes beneficios.

Si reconoces en ti las siguientes características, entonces ¡no hay duda de que lo eres!, pero para saberlo responde el siguiente test con los que mejor se adecúen a ti.

Te adaptas fácilmente al uso de nuevos materiales digitales.		
Eres parte de foros y comunidades online de educadores.		
Más que un maestro tradicional qué explica los libros, eres un coach motivador para tus alumnos.		
Utilizas las redes sociales como herramienta pedagógica aprovechando para enseñar sobre como protegerse en linea.		
Los sitios web y aplicaciones móviles son tus herramientas educativas.		
Acuerdas con las madres, padres y cuidadores las reglas de uso de Internet y dispositivos en clase.		
Enseñas a tus estudiantes a usar los buscadores y a ser críticos a la hora de seleccionar información.		
Enseñas a tus estudiantes a respetar la privacidad en Internet y a respetar los derechos de los demás.		

Conoce tus resultados

Adaptarte al mundo digital puede ser algo complicado, sin embargo, el uso de las TIC dentro de las instituciones educativas es una realidad, conocerlas, aplicarlas y enseñar su uso seguro más allá de lo recreativo es vital y nosotros te acompañaremos en el proceso.



7 - 8
Eres un docente 2.0

Eres todo un docente 2.0 lo que sin duda te convierte en todo un defensor digital de tu institución educativa, implementar herramientas digitales y enseñar su uso seguro es lo tuyo, ahora solo falta compartir tus conocimientos, ademas de apoyar a tus estudiantes, apoya a tus compañeros docentes que se estén adaptando a la tecnología, crear comunidades ciberseguras es tarea de todos.

4 - 6
Un estirón más

Vas por buen camino, comienzas poco a poco a implementar las TIC dentro de tu aula, además de involucrar a un número aún más grande de personas a usarlas de forma adecuada y segura. Es un gran paso para convertirte en un docente 2.0.

0 - 3
Debes iniciar

El bombardeo tecnológico puede ser muy abrumador y mantenerte actualizado puede ser complejo, sin embargo nunca es tarde para comenzar a incursionar en el mundo digital y guiar a tus estudiantes, recuerda que hablar de tecnología con las NNA pueden generar un gran equipo para la enseñanza mutua.

Información para comenzar

Iniciemos tu preparación Docente 2.0

Los estudiantes se han desarrollado en un contexto digital por lo que el profesorado debe adecuarse a su forma de actuar y de concebir el aprendizaje, de igual forma el docente también debe digitalizarse (conocer el entorno digital), de tal forma que pueda construir una respuesta colectiva a los retos que hoy plantea la educación en el panorama digital, así pues, los docentes, al igual que el alumnado, deben aprender a ser competentes digitales, pero más importante aún, deben resignificar y adaptar su competencia docente a un mundo digitalizado.

Es por lo anterior que **queremos darte algunos consejos que te permitirán conocer lo que involucra la vida digital y cómo convertirte en todo un defensor digital dentro de tu institución educativa** y ayudar a prevenir riesgos en tus estudiantes.

Potenciar las oportunidades para reducir los riesgos

Internet ha cambiado el mundo, por tanto, ha cambiado la forma de transitar la infancia y la adolescencia, para bien o para mal, la tecnología digital se encuentra ya en medio de nuestras vidas, nuestro deber es abogar por potenciar los aspectos positivos de Internet en la vida de las NNA y disminuir los riesgos en la interacción con el ciberespacio. Lo que se traduce en acciones prioritarias que reconozcan la responsabilidad que compartimos de proteger a NNA contra los peligros del mundo digital.

1 Proporcionar a todas las NNA acceso a dispositivos digitales y conectividad.

El acceso digital es un factor cada vez más determinante para la igualdad de oportunidades de las NNA, al facilitar que se beneficien del acceso a la información, el conocimiento, la participación comunitaria y el compromiso social.

Si bien, no es posible muchas veces que cada niña, niño o adolescente cuente con algún dispositivo electrónico propio para usar dentro del aula o incluso en su hogar, es importante brindar la oportunidad a cada NNA de tener acercamientos con la tecnología, su funcionamiento y uso, ya sea por medio de algún dispositivo con conexión a Internet para cada salón o creando dinámicas que permitan trabajos en equipo para compartir dispositivos.

2 Alfabetización digital para las NNA.

Las niñas, niños y adolescentes de hoy son nativos digitales, pero eso no significa que no necesiten orientación y apoyo para aprovechar al máximo la conectividad, considerando que en la mayoría de los casos no entienden automáticamente su vulnerabilidad a los riesgos en línea, o su propia responsabilidad de ser buenos ciudadanos digitales.

2.1 Tecnología en preescolar

En la educación inicial las TIC son una herramienta pedagógica muy importante ya que permite que las niñas y niños se familiaricen con la tecnología de manera segura y supervisada, sin embargo, **el uso de la tecnología en niños menores de 8 años es un tema debatido en el desarrollo infantil, pues se recomienda limitar su uso en niños pequeños.**

Desarrollo cognitivo y emocional: Los niños menores de 8 años están en una etapa crítica de desarrollo cognitivo y emocional, necesitan interactuar con su entorno físico y social para aprender habilidades importantes, el uso excesivo de la tecnología puede interferir con estas experiencias vitales y afectar negativamente su desarrollo.

Retraso del desarrollo motor: El uso prolongado de dispositivos electrónicos puede limitar las oportunidades de juego activo y movimiento físico en los niños pequeños.

Problemas de salud: El uso excesivo de la tecnología en niños pequeños puede estar asociado con problemas de salud, como obesidad, trastornos del sueño, problemas de visión y problemas posturales.

Contenido inapropiado: Los niños menores de 8 años pueden no tener la capacidad de comprender completamente el contenido en línea y pueden estar expuestos a contenido inapropiado o perjudicial, como violencia, pornografía o mensajes engañosos.

Interferencia en las relaciones sociales: El uso excesivo de la tecnología puede afectar las habilidades sociales y de comunicación en los niños pequeños, ya que pueden perder oportunidades para interactuar cara a cara con otros niños y adultos.

2.2 Tecnología en primaria y secundaria

Es recomendable guiar sobre el manejo de conceptos y funciones básicas asociadas a las TIC que permita una mayor apropiación, el uso de la tecnología en las escuelas pueden ofrecer varios beneficios.

Acceso a información y recursos: La tecnología permite a los estudiantes acceder a una amplia gama de información y recursos en línea, lo que puede enriquecer su aprendizaje, ampliar sus horizontes y brinda la oportunidad de explorar y aprender de manera autónoma.

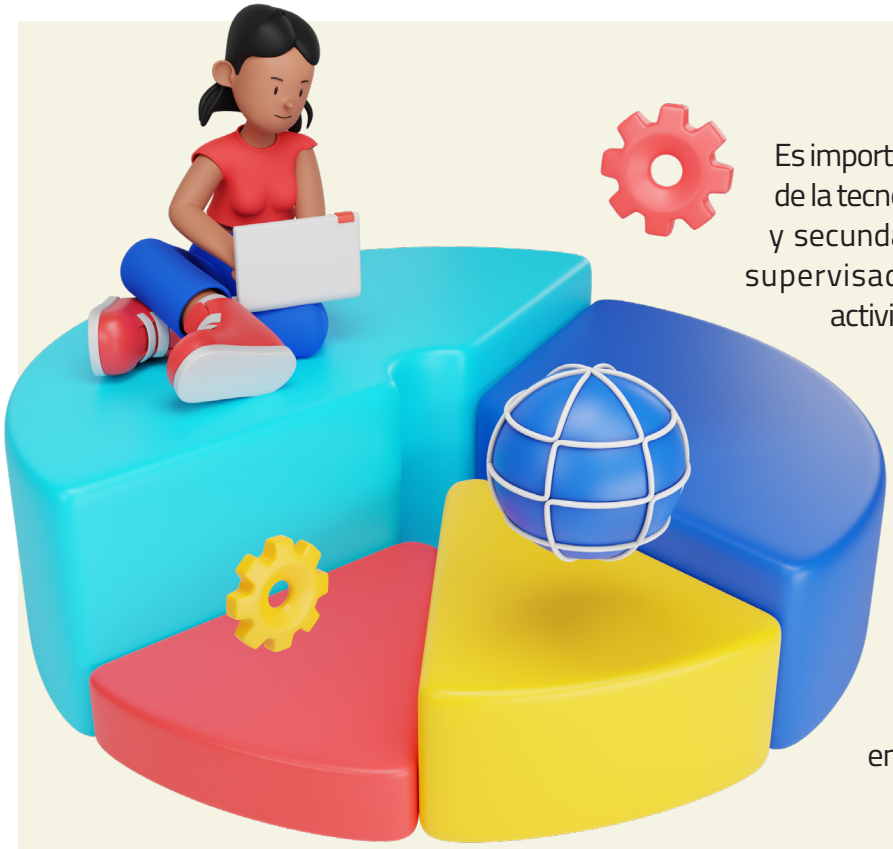
Mejora del aprendizaje: La tecnología puede facilitar y enriquecer el proceso de aprendizaje, ofrece recursos educativos en línea, aplicaciones interactivas y herramientas de colaboración que pueden ayudar a los estudiantes a adquirir conocimientos y habilidades de manera más efectiva y motivadora.

Fomento de habilidades digitales: La tecnología puede ayudar a desarrollar habilidades digitales en los estudiantes, pueden aprender a usar aplicaciones, navegadores web, herramientas de procesamiento de texto además de otras herramientas digitales de forma adecuada y segura, lo que los prepara para el mundo digital en constante evolución.

Personalización del aprendizaje: Los estudiantes pueden acceder a recursos y actividades que se ajusten a su nivel de habilidad, estilo de aprendizaje y ritmo de trabajo, lo que puede ayudarlos a avanzar a su propio ritmo y alcanzar su máximo potencial.

Mejora de la comunicación y la retroalimentación: La tecnología puede facilitar la comunicación entre estudiantes y maestros, así como la retroalimentación sobre el progreso del aprendizaje, los estudiantes pueden utilizar plataformas en línea para comunicarse con sus maestros, recibir retroalimentación sobre sus tareas, proyectos, y colaborar con sus compañeros de clase.

Preparación para el futuro: El uso de la tecnología puede ayudar a preparar a los estudiantes para el mundo laboral y social del futuro,las habilidades digitales son cada vez más demandadas en la mayoría de los campos profesionales, familiarizarse con la tecnología desde una edad temprana favorece a los estudiantes a crear una base sólida para su futuro académico y profesional.



Es importante tener en cuenta que el uso de la tecnología en las escuelas primarias y secundarias debe de ser adecuado, supervisado y equilibrado con otras actividades educativas y recreativas, los docentes,madres, padres y cuidadores deben supervisar que el uso de los recursos tecnológicos sea apropiado para la edad de los estudiantes que se encuentren alineados con los objetivos educativos, se promueva un uso responsable y seguro de la tecnología en el entorno escolar.

2.3 Tecnología en preparatoria y universidad

Los adolescentes utilizan con gran facilidad las TIC, por lo que es importante difundir acciones para mantenerse ciberseguros y explotar de forma responsable estas herramientas.

Mejora de la participación y la motivación: El uso de tecnología en el aula puede hacer que el aprendizaje sea más atractivo y participativo para los estudiantes, herramientas digitales como vídeos, aplicaciones educativas, simulaciones y juegos interactivos, pueden ayudar a motivar a los estudiantes y hacer que el proceso de aprendizaje sea más interesante y entretenido.

Preparación para la educación superior y el mundo laboral: Muchas instituciones educativas y empleadores requieren habilidades tecnológicas en la actualidad, su uso puede ayudar a los estudiantes a desarrollar habilidades que les sean útiles en su futura vida académica y profesional.

3 Proteger a las NNA de los daños en línea

La era digital aumentó los riesgos existentes para las NNA y creó otros nuevos, la materialización de un incidente puede ser devastador y cambiarles la vida, es probable que los adolescentes tengan una mayor capacidad de adaptabilidad a la era digital y sientan a veces el deseo de incursionar más en la vida digital, tal curiosidad es necesaria para que estos aprendan a adaptarse y a desarrollar resiliencia.

Ayudar a las personas que apoyan a las NNA. De manera conjunta se debe trabajar con madres, padres y cuidadores para desarrollar las capacidades necesarias para mediar de manera positiva en el uso de las TIC por parte de NNA, en lugar de simplemente restringirlo.

4 Proteger la privacidad y la identidad de las NNA en línea

La máxima protección de la privacidad debe ser la configuración básica de las herramientas y plataformas digitales utilizadas por niñas, niños y adolescentes por lo que la privacidad debe incluirse en el diseño de las nuevas tecnologías desde un inicio.

Competencias digitales para Docentes

Las competencias digitales son el conjunto de conocimientos y habilidades que permiten un uso seguro y eficiente de las tecnologías de la información y las comunicaciones (TIC).

Alfabetización Digital

Identificar, almacenar y gestionar contenidos digitales de mayor relevancia para el ejercicio de la docencia.

Comunicación y Colaboración

Utilizar tecnologías para el trabajo en equipo, colaboración en la creación de contenidos, recursos y construcción de conocimientos.

Creación de Contenidos Digitales

Diseñar contenido original y relevante (vídeos, presentaciones e imágenes) en diferentes formatos y espacios como webs, blogs, canales de YouTube entre otros, procurando el desarrollo de competencias digitales del alumnado.

Seguridad

Comprender las diferentes amenazas que existen en la red y adoptar medidas de ciberseguridad para la protección de datos.

Resolución de Problemas

Identificar necesidades y adaptar herramientas y recursos digitales para asignar posibles soluciones procurando el empoderamiento positivo del alumnado.

5 Claves para ser un docente innovador

UTILIZA las TIC en el aula como instrumento de trabajo más allá de su uso como entretenimiento.

COMBINA diferentes tipos de trabajo y agrupamiento de los estudiantes para mejorar la convivencia.

DEJA al estudiante que sea el protagonista de su propio aprendizaje.

INVOLUCRA en el proceso de aprendizaje al núcleo familiar.

SIGUE varios procesos de enseñanza-aprendizaje hacia el desarrollo de las inteligencias múltiples y la sana convivencia.

Comenzar a involucrar las TIC dentro del aula con un enfoque sano de uso así como su convivencia dentro y fuera del mundo digital, marcara diferencias sobre el impacto en el que las nuevas tecnologías conviven en el desarrollo de las NNA.

Comencemos
con la Alfabetización Digital

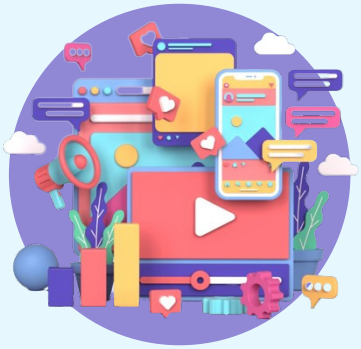
¿Qué es?

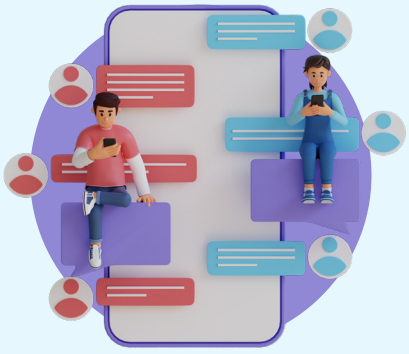
La alfabetización digital se refiere a la capacidad de una persona para **utilizar, comprender, evaluar y participar de manera efectiva en el mundo digital,** implica tener habilidades y conocimientos para interactuar con la tecnología de **forma responsable, crítica y segura,** es esencial para que las NNA puedan navegar de manera segura.

La alfabetización digital ayuda a las NNA en varios aspectos importantes.

Acceso a la información:

Permite acceder a una amplia gama de información en línea, lo que puede enriquecer su aprendizaje, así como la adquisición de conocimiento en diversos temas, también permite buscar información con lo que permite evaluar su calidad, confiabilidad, y utilizarla de forma adecuada.





Comunicación y colaboración:

Ayuda a desarrollar habilidades de comunicación efectiva en línea, incluyendo la escritura, la participación en redes sociales, la colaboración en proyectos en línea y el uso de herramientas de comunicación digital.

Pensamiento crítico y resolución de problemas:

La alfabetización digital fomenta el desarrollo del pensamiento crítico y la habilidad para resolver problemas en un entorno digital, las NNA aprenden a evaluar la información en línea, a identificar noticias falsas o desinformación, a analizar situaciones en línea y a tomar decisiones informadas y responsables en el uso de la tecnología.

Seguridad en línea:

Incluye el conocimiento y las habilidades para proteger su privacidad, permite que entendamos los riesgos en línea y la forma en como podemos protegernos, como utilizar contraseñas seguras, cambiar la privacidad de nuestra información personal para navegar de manera segura en el ciberespacio.

Ciudadanía digital:

La alfabetización digital también implica seguir normas y valores éticos en línea, NNA aprenden sobre la responsabilidad digital, el respeto a los demás en línea, la importancia de la diversidad y la inclusión en el mundo digital para contribuir de manera positiva en un entorno digital.

Alfabetización digital para adultos, ¿en qué nos beneficia?

Empleabilidad:

Nos ayuda a adquirir habilidades digitales necesarias para utilizar herramientas de productividad digital de modo que podamos colaborar en entornos de trabajo digitales, lo que puede aumentar las oportunidades de empleo y progreso profesional.

Comunicación y conectividad:

Permite mantenerse conectados con sus seres queridos, amigos y colegas a través de plataformas de redes sociales y mensajería instantánea, también nos permite acceder a información, servicios y recursos en línea para la vida cotidiana, como la banca en línea, compra en línea y búsquedas de interés.

Acceso a información:

Ahora podemos tomar decisiones informadas sobre temas como salud, educación, finanzas y comercio electrónico.

Participación cívica y social:

Nos permite participar de manera activa en la comunidad digital, ya sea a través de participación en discusiones en línea, firma de peticiones, difusión de causas sociales y la participación activa en ejercicios comunitarios en linea.

En términos generales la alfabetización digital incluye poseer conocimiento de diversas fuentes de información digitales, criterios éticos para hacer uso de la información para priorizar nuestra seguridad, por lo que Guillén, Ascencio y Tarango (2016), clasifican cinco dimensiones de este aprendizaje:

1. **INSTRUMENTAL:**
Se refiere al conocimiento práctico y habilidades para el uso del hardware y software.

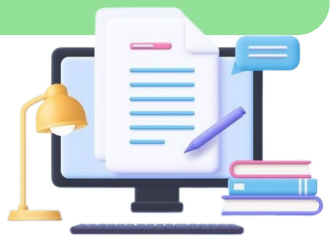
2. **COGNITIVO-INTELECTUAL:**
Trata de los conocimientos y habilidades cognitivas específicas que permitan buscar, seleccionar, analizar, interpretar y recrear información con la finalidad de otorgarle significado, analizarla críticamente y reconstruirla.

3. **AXIOLÓGICA:**
Plantea la toma de conciencia en cuanto a que las TIC inciden significativamente en el entorno cultural y político de la sociedad, así como a la adquisición de valores éticos y democráticos con relación al uso de la información.

4. **SOCIOCOMUNICACIONAL:**
Relativa a la habilidad para comunicarse eficazmente a través de las TIC, mediante el desarrollo de textos de naturaleza diversa, además, está dimensión incluye el desarrollo de normas de comportamiento que impliquen una actitud social positiva hacia los demás como puede ser el trabajo colaborativo, el respeto y sobre todo una empatía en redes.

5. **EMOCIONAL:**
Relativa al conjunto de afectos, sentimientos y pulsiones emocionales provocadas por la experiencia en los entornos digitales para el control de las emociones, el desarrollo de empatía para la construcción de una identidad digital caracterizada por el equilibrio afectivo-personal en el uso de las TIC.

Con todo esto podemos acceder a los beneficios sociales, culturales y económicos que las TIC ofrecen.



¿Qué se necesita para implementar la alfabetización digital?

La implementación de la alfabetización digital en las escuelas puede llevarse a cabo de varias formas, dependiendo del nivel educativo y los recursos disponibles. **Aquí hay algunos ejemplos sobre que se necesita para implementar la alfabetización digital en las escuelas:**

Incorporar la tecnología en el currículo: Los docentes pueden integrar la tecnología de manera activa en el currículo, utilizando herramientas digitales para la enseñanza y el aprendizaje de diferentes materias.

Acceso a dispositivos y conectividad: Es importante garantizar que los estudiantes tengan acceso a dispositivos digitales, como computadoras, tabletas o dispositivos móviles, así como a una conexión a Internet confiable, esto les permitirá practicar y desarrollar habilidades digitales en un entorno real.

Integrar proyectos y actividades prácticas: Los proyectos y actividades prácticas pueden ser una forma efectiva de fomentar la alfabetización digital en las escuelas.

Enseñar habilidades de búsqueda y evaluación de información en línea: La alfabetización digital también implica enseñar a los estudiantes cómo buscar, evaluar y utilizar información en línea de manera crítica y responsable.

Fomentar la seguridad en línea y la ciudadanía digital: La alfabetización digital también incluye enseñar a los estudiantes sobre la seguridad en línea, la privacidad, la protección de datos y la ciudadanía digital responsable.

Actividades que puedes utilizar en clase para impartir una alfabetización digital

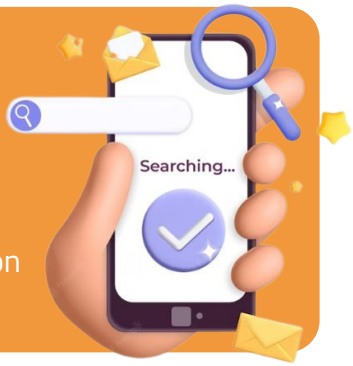
Búsqueda de información en línea

Los estudiantes pueden practicar la búsqueda de información en línea utilizando motores de búsqueda y navegando por diferentes sitios web para encontrar información relevante sobre un tema específico, luego, pueden evaluar la calidad de la información encontrada y discutir en clase cómo determinar si una fuente en línea es confiable o no.

Pueden hacer preguntas como:

- **¿Quién escribió esto?**
- **¿Cuál es su experiencia o autoridad en el tema?**
- **¿Hay evidencia o referencias para respaldar la información?**

Esto ayudará a desarrollar habilidades críticas de evaluación de la información en línea.



Creación de presentaciones multimedia

Los estudiantes pueden crear presentaciones multimedia utilizando herramientas digitales como PowerPoint, Google Slides o Prezi, pueden aprender a insertar imágenes, videos, enlaces y otros elementos multimedia en sus presentaciones, editar y comentar documentos en tiempo real, por lo que pueden colaborar de modo efectivo en un entorno digital.

Creación de contenido digital original

Los estudiantes pueden crear su propio contenido digital original, como blogs, videos, podcasts o presentaciones multimedia, para desarrollar habilidades de creación de contenido digital y entender cómo compartir y publicar contenido de manera ética y responsable.

Actividades de codificación o programación

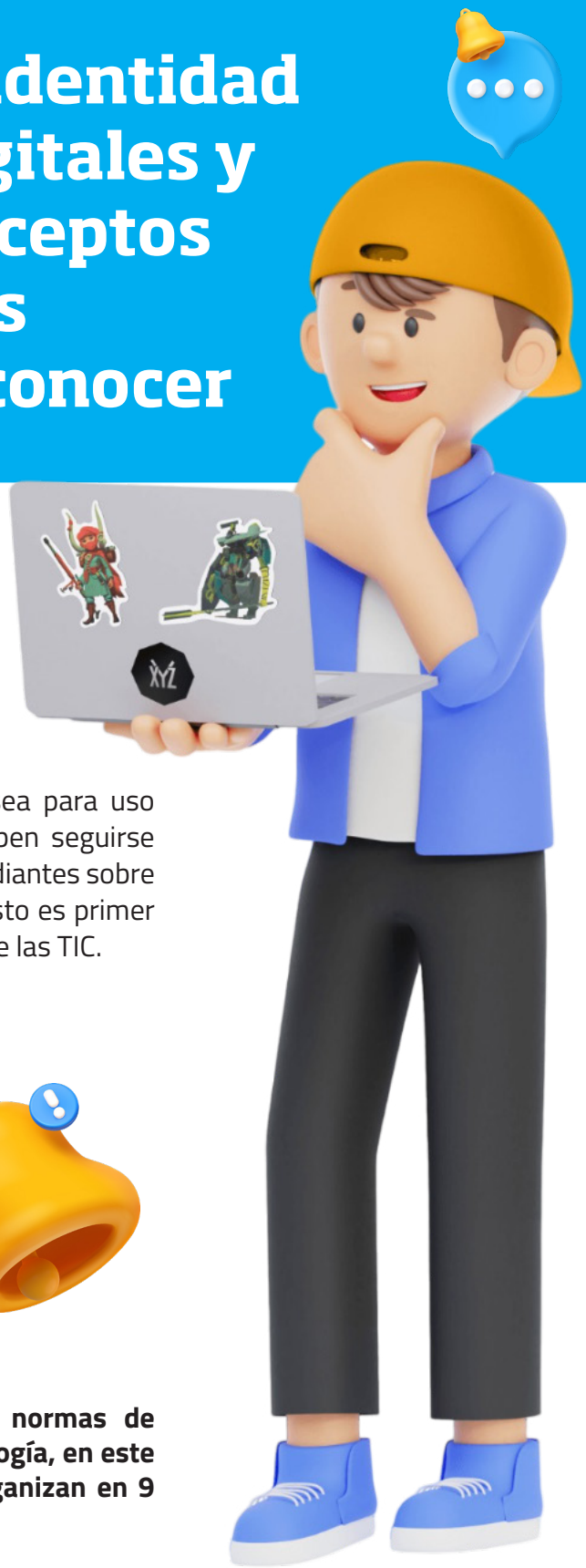
Los estudiantes pueden crear su propio contenido digital original, como blogs, videos, podcasts o presentaciones multimedia, para desarrollar habilidades de creación de contenido digital y entender cómo compartir y publicar contenido de manera ética y responsable.

Actividades de codificación o programación

Los estudiantes pueden participar en actividades de codificación o programación utilizando herramientas y recursos en línea, como Scratch, Code.org o plataformas de aprendizaje de programación, esto les permitirá desarrollar habilidades de pensamiento lógico y resolución de problemas, así como comprender los conceptos básicos de la programación.

Estos son solo algunos ejemplos de ejercicios que se pueden utilizar en clase para iniciar a impartir alfabetización digital, es importante adaptar las actividades a las necesidades y nivel de los estudiantes, así como a los recursos tecnológicos disponibles en el entorno educativo, no olvides informar sobre las normas de uso de las TIC y sus riesgos.

Ciudadanía digital, identidad digital, derechos digitales y ciberseguridad, conceptos primordiales que tus estudiantes deben conocer



La Ciudadanía Digital

El uso de las TIC dentro y fuera de las aulas, ya sea para uso educativo o recreativo trae consigo normas que deben seguirse para lograr un sano espacio digital, habla con tus estudiantes sobre ciudadanía digital, su importancia e impacto social, esto es primer paso para generar conciencia sobre el uso favorable de las TIC.

La ciudadanía digital puede definirse como las normas de comportamiento que conciernen al uso de la tecnología, en este caso dentro y fuera del aula, estas normas se organizan en 9 áreas de comportamiento.

1 Netiqueta:

Etiqueta, estándares de conducta o manera de proceder con medios electrónicos.

Las normas de comportamiento en la red y sus modelos deben inspirar al los estudiantes, sin embargo, en algunos casos las pautas de actuación no están escritas todavía o bien no están consensuadas por todos los usuarios, por lo que a medida que las tecnologías proliferan, los usuarios adoptan unas formas de utilización que no siempre suponen un uso adecuado.

Ejemplo negativo de esta área:

Los estudiantes mandan y reciben mensajes desde sus dispositivos que no tienen ninguna relación con el trabajo desarrollado durante la clase.

Estrategias para esta área de comportamiento

- **Seguir las reglas y políticas establecidas por la escuela para el uso adecuado de la tecnología.**
- **Utilizar casos o escenarios para ilustrar formas adecuadas e inadecuadas para utilizar la tecnología.**
- **Diseñar modelos de uso adecuados de la tecnología dentro y fuera del aula.**

2 Comunicación:

Intercambio electrónico de información.

Las TIC han transformado las formas en las que se comunican las personas, creando una nueva estructura social de quién, cómo y cuándo, interactúan las personas. **Los estudiantes deben aprender a diferenciar cuál es la forma de comunicación adecuada para una circunstancia determinada,** por ejemplo, la comunicación cara a cara es más efectiva que la comunicación electrónica cuando los temas que se van a tratar involucran información delicada, personal o negativa, mientras que la comunicación electrónica es eficiente y efectiva para trasmitir información básica.

Ejemplo negativo de esta área:

Los estudiantes usan el móvil como una forma para excluir a otros de grupos privados en redes sociales o dentro de su lista de contactos.

Estrategias para esta área de comportamiento

- Modelar el uso adecuado de la comunicación electrónica.
- Incentivar el uso de teléfonos móviles con propósitos educativos, por ejemplo, para acceder a información en tiempo real en la resolución de dudas.

3 Educación:

El proceso de enseñar y aprender sobre tecnología.

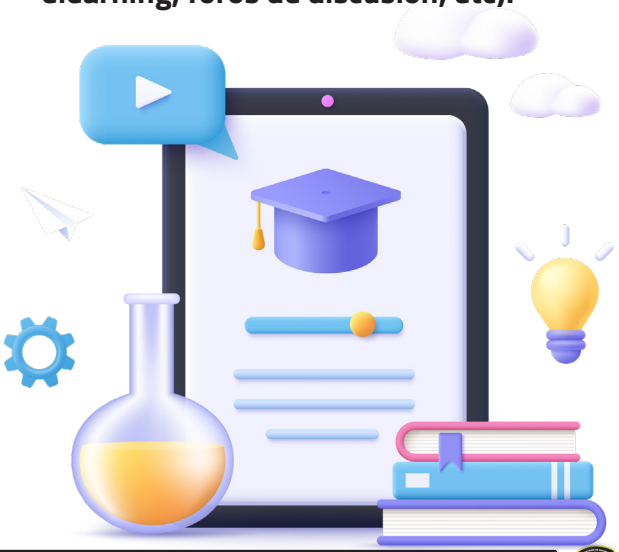
Ejemplo negativo de esta área:

Los estudiantes utilizan sus dispositivos para que les pasen las respuestas en exámenes.

Los docentes no enseñan a los estudiantes cómo utilizar la tecnología para encontrar recursos y materiales fiables.

Estrategias para esta área de comportamiento

- Incentivar a los estudiantes a que encuentren usos nuevos y alternativos para Internet y otras tecnologías digitales.
- Ofrecer oportunidades de aprendizaje en las que se utilicen distintas facetas de la tecnología (ej: sitios web, plataformas de elearning, foros de discusión, etc).



4 Acceso: Participación electrónica plena en la sociedad.

Ejemplo negativo de esta área:

Los docentes evitan realizar proyectos o tareas que involucren el uso de la tecnología por temor a que los estudiantes no cuenten con acceso a ello.

La escuela ignora o subestima las necesidades tecnológicas de grupos marginados.

La escuela fracasa en compensar a los estudiantes que no tienen acceso a la tecnología en sus casas.

Estrategias para esta área de comportamiento

- Identificar estudiantes que tengan circunstancias y necesidades especiales y explorar formas de acomodarlos o buscar alternativas a sus necesidades tecnológicas.
- Ofrecer tiempo en la escuela, a los estudiantes que no tienen acceso en su hogar, para que puedan utilizar la tecnología con el fin de realizar trabajos académicos.
- Planificar actividades en las que trabajen en binomios para la resolución de tareas, en la que un integrante cuente con acceso a las TIC.

5 Responsabilidad:

Por hechos y acciones en los medios electrónicos.

Es fácil encontrar estudiantes de Secundaria, Bachillerato o incluso Universidad que utilizan software comercial sin licencia o descargados de forma ilegal, **sin tener ninguna conciencia de haber hecho nada ilegal.**

Ejemplo negativo de esta área:

Para proyectos de clase, los estudiantes copian material de Internet y no reconocen la autoría del mismo.

El alumnado utiliza software comercial con licenciamiento no fidedigno.

Estrategias para esta área de comportamiento

- Promover entre los estudiantes un diálogo en el que se discuta lo que ellos sienten cuando los materiales que ellos han realizado se descargan sin su permiso.
- Dialogar con los estudiantes sobre el código de conducta del colegio y sobre otras leyes específicas que se relacionen con el uso ilegal de las tecnologías y las consecuencias o los costos de no respetar esas reglas o leyes.
- Fomentar la discusión sobre las percepciones de los estudiantes respecto al uso ético y no ético de la tecnología.

6 Comercio:

Compraventa electrónica de bienes y servicios.

Comprar en línea es una práctica frecuente y los estudiantes deben entender de qué se trata, si nuestro objetivo es la formación de ciudadanos digitales, entonces **tratar el comercio electrónico es importante.**

Ejemplo negativo de esta área:

Los estudiantes realizan compras en línea sin saber cómo proteger adecuadamente sus datos.

Estrategias para esta área de comportamiento

- Estimular la participación de los estudiantes en una discusión en la que se expongan experiencias buenas y malas de las compras en línea.
- Enseñar a los estudiantes el peligro que tiene el robo de identidades y de qué manera pueden protegerse.
- Identificar elementos que resultan de una pagina apócrifa y no confiable.

7 Derechos:

Las libertades que tienen todas las personas en el mundo digital.

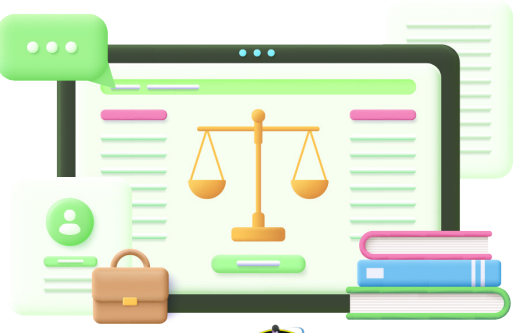
Ejemplo negativo de esta área:

Los estudiantes violan las políticas de uso establecidas por la escuela porque las perciben como injustas.

La institución no protege los derechos de los usuarios que trabajan con la tecnología de la escuela.

Estrategias para esta área de comportamiento

- Informar a los docentes sobre los derechos digitales de los estudiantes.
- Informar a los estudiantes sobre sus derechos digitales, puedes apoyarte echando un vistazo a la siguiente pagina: **https://www.unicef.es/infancia-tecnologia**
- Fomentar la discusión por parte de la comunidad escolar de las razones para el establecimiento de políticas respecto a la tecnología.



8 Ergonomía:

Bienestar físico en un mundo tecnológico digital.

Los estudiantes deben estar conscientes de los **daños físicos que puede ocasionar el abuso de la tecnología,** el síndrome del túnel carpiano, el forzar la vista y la mala postura son problemas comunes en las actividades relacionadas con la tecnología.

Ejemplo negativo de esta área:

Los docentes no enseñan ergonomía cuando los estudiantes utilizan la tecnología.

Estrategias para esta área de comportamiento

- Asegurarse de que las aulas están bien iluminadas y que el mobiliario es el adecuado para usar la tecnología en forma segura.
- Informar al alumnado de los problemas físicos a largo plazo que pueden generar ciertos usos inadecuados de la tecnología.

9 Riesgo (auto protección):

Precauciones para garantizar la seguridad en los medios electrónicos.

Cada vez se guarda mayor cantidad de información de carácter confidencial en los dispositivos, por lo que se deben generar estrategias para protegerla, **los estudiantes deben aprender a proteger sus datos** respondiendo a la necesidad de cuidar a la comunidad.

Ejemplo negativo de esta área:

- **Los estudiantes y docentes asumen que no hay ninguna necesidad de proteger los datos electrónicos.**
- **Los alumnos no protegen su identidad cuando usan correos electrónicos, participa en salas de chats, etc.**

Estrategias para esta área de comportamiento

- Ponerse en contacto con instituciones especializadas como la Policía Cibernética del Municipio de San Luis Potosí para obtener materiales que le indiquen cómo protegerse.
- Enseñar a los estudiantes, cómo verificar infecciónes por malware o cualquier campaña maliciosa que pueda surgir.

Identidad Digital otro tema del que hablar

¿Qué es?

La Identidad Digital es el conjunto de información publicada en Internet sobre mí, datos personales, imágenes, comentarios, gustos, amistades, aficiones, etc. Todos estos datos me describen en Internet ante los demás y pueden componer la imagen que los demás tienen sobre mi.

Esta identidad puede construirse sin que corresponda exactamente con la realidad, sin embargo lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

La identidad digital es ...

- SOCIAL
- SUBJETIVA
- VALIOSA
- INDIRECTA
- COMPUESTA
- REAL
- DINÁMICA

Se construye navegando por las redes sociales a partir del reconocimiento de los demás sin ni siquiera llegar a comprobar si esa identidad es real o no.

Depende de cómo los demás perciban a esa persona a través de las informaciones que genera.

A veces personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre este.

No permite conocer a la persona directamente sino las referencias publicadas de esa persona.

La identidad digital se construye por las aportaciones de la misma persona y también por otras personas sin la participación o consentimiento del mismo.

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

La identidad digital no es una foto instantánea sino que está en constante cambio o modificación.

6 Consejos para una buena Identidad Digital

(PARA ESTUDIANTES Y DOCENTES)

Una identidad digital bien gestionada no sólo repercute en una vida más activa en todos los ámbitos sino que también tiende a consolidar un entramado social más sólido fuera de Internet.

Creación responsable de perfiles en las redes sociales.
Pensar qué datos se van a a publicar en ese perfil y en ocasiones diferenciar entre perfil personal y perfil laboral/académico.

Configuración adecuada de la seguridad y privacidad.
Definir de forma correcta las opciones de privacidad del perfil en las redes sociales, pensar si el contenido a subir es apropiado para difundir en público o sólo en el círculo de amistades.

Participación agradable en la Red.
No utilizar un tono maleducado o vejatorio, mostrar tolerancia y empatía hacia los demás, no difundir información falsa, pedir permiso a las personas que aparecen en fotos o vídeos antes de subirlas, ser respetuoso en el empleo de etiquetas en fotos y vídeos.

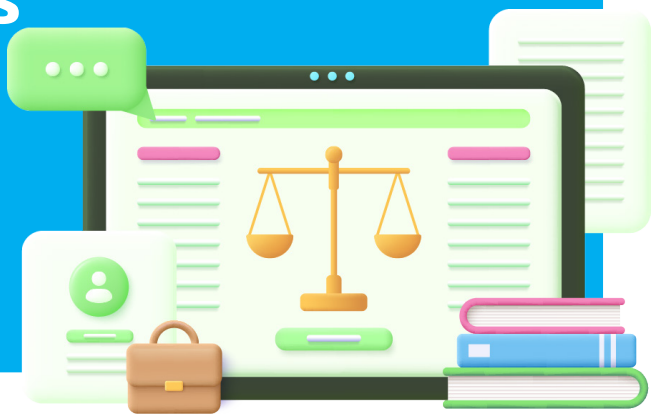
Medidas de seguridad en la navegación.
Mantener actualizado el sistema operativo, antivirus y software.

Revisión periódica de la identidad.
Utilizar los buscadores para controlar cada cierto tiempo la información disponible sobre sí mismo en Internet y en especial en las redes sociales.

Ayuda.
Es necesario buscar ayuda cuando sospeches que alguien está dañando tu identidad y reputación online mediante la suplantación de identidad, sextorsión, ciberacoso, etc.

Los Derechos Digitales

Son un conjunto de garantías que protegen la libertad, privacidad, seguridad e igualdad en el entorno digital. Así pues, son extensión de los derechos humanos tradicionales a la era digital, reconociendo la importancia de la tecnología en la vida cotidiana y la necesidad de proteger a los usuarios en línea.



Es importante destacar que los derechos digitales son universales y se aplican a todas las personas, independientemente de su género, raza, orientación sexual, religión o cualquier otra característica personal, además, estos derechos deben ser protegidos y garantizados por los gobiernos.

¿Cuáles son ?

Los derechos digitales de las niñas, niños y adolescentes son una extensión de los derechos humanos universales que se aplican al uso de las tecnologías digitales. Estos derechos incluyen:

1 **PRIVACIDAD:**
La privacidad es vital para la capacidad de acción, la dignidad y la seguridad de los niños y para el ejercicio de sus derechos.

2 **LIBERTAD DE EXPRESIÓN:**
El derecho de las NNA a la libertad de expresión incluye la libertad de buscar, recibir y difundir información e ideas de todo tipo, utilizando cualquier medio de su elección.

3 **DERECHO A LA EDUCACIÓN:**
El entorno digital puede facilitar y mejorar en gran medida el acceso de los niños a una educación inclusiva de alta calidad, incluidos recursos fiables para el aprendizaje formal, no formal, informal, entre pares y autodirigido.

4 **PROTECCIÓN CONTRA LA EXPLOTACIÓN SEXUAL Y LA TRATA DE PERSONAS:**
Se debe proteger a los niños de todas las formas de explotación perjudiciales para cualquier aspecto de su bienestar en relación con el entorno digital.

5

DERECHO A LA PARTICIPACIÓN:

Las niñas, niños y adolescentes tienen derecho a participar en la toma de decisiones sobre su uso de las tecnologías digitales.

6

ACCESO A LA INFORMACIÓN:

Se debe garantizar que las NNA tengan acceso a una amplia diversidad de información digital, incluida la información en poder de organismos públicos, sobre cultura y deportes., las artes, la salud, los asuntos civiles y políticos y los derechos del niño.

7

PROTECCIÓN CONTRA EL ACOSO CIBERNÉTICO Y LA VIOLENCIA EN LÍNEA:

Se deben adoptar medidas legislativas para proteger a las NNA de los riesgos reconocidos y emergentes de todas las formas de violencia en el entorno digital.

Es importante destacar que estos son solo algunos de los principales derechos digitales, y que la lista puede variar dependiendo de la región, el país y la cultura. En general, los derechos digitales buscan garantizar que las personas puedan disfrutar de las mismas libertades y protecciones en línea que en el mundo físico.

¿POR QUÉ ES IMPORTANTE DARLOS A CONOCER?

Es importante enseñar a niñas, niños y adolescentes sobre sus derechos digitales porque la tecnología digital se ha convertido en una parte fundamental de la vida cotidiana. Las NNA son cada vez más activos en línea, ya sea a través de las redes sociales, los juegos en línea o la búsqueda de información en la web.

Al mismo tiempo, hay muchos riesgos asociados con el uso de la tecnología digital, como el acoso cibernético, la exposición a contenidos inapropiados, la pérdida de privacidad y el robo de identidad. Por lo tanto, **es importante que las NNA conozcan sus derechos digitales para que puedan protegerse y disfrutar de un uso seguro y responsable de la tecnología.**

Ciberseguridad otro concepto fundamental

El término ciberseguridad hace referencia a la ausencia de peligro que se logra alcanzar en las TIC, es decir, es la práctica de proteger tu información digital, dispositivos y activos, esto incluye información personal, cuentas, archivos, fotos e incluso el dinero.

6 CONSEJOS PARA ESTUDIANTES Y DOCENTES PARA MEJORAR SU SEGURIDAD DIGITAL

Los siguientes consejos son los mejores para comenzar a enseñar a tus estudiantes seguridad digital, enseñarlos de manera ejemplificada y llevándolo a cabo de manera grupal facilitará su entendimiento y aplicación.

1 BUENAS CONTRASEÑAS:

Una buena contraseña es única, fácil de recordar para ti y difícil de adivinar para los demás, debe contener símbolos especiales, (#%_"?!).

2 USA LA VERIFICACIÓN EN DOS PASOS:

Hace más seguras tus cuentas y mucho mas difícil para otros acceder de manera indebida.

3 NO REVELES TU UBICACIÓN:

Muchos servicios tienen acceso a tu ubicación, revoca los permisos y nunca compartas tu ubicación en redes sociales.

4 CUIDADO CON LO QUE AUTORIZAS:

No hagas clic en enlaces que te pidan autorizar el acceso a tus redes sociales, que confirmes o compartas información.

5 USA HTTPS:

HTTPS permite establecer una conexión segura que no puede ser interceptada por personas no autorizadas.

6 TEN CUIDADO CON LO QUE PUBLICAS:

Recuerda que lo que publiques en Internet no desaparecerá nunca, debes ser cuidadoso con lo que estas dispuesto a compartir.

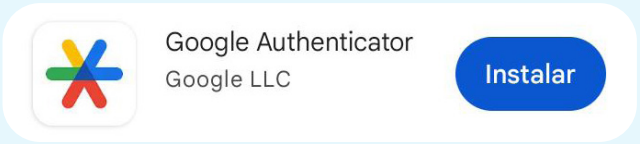
HERRAMIENTA DIGITAL

¿VERIFICACIÓN QUE?...

Docente, la verificación en dos pasos es un mecanismo de protección adicional a la hora de iniciar sesión en nuestras cuentas online, evitando que alguien sin autorización acceda a tus cuentas o las cuentas de NNA, **te enseñamos como pueden instalarla tu y tus estudiantes.**

1 Para comenzar.

Te enseñaremos cómo usar la verificación en dos pasos, primero **descarga la aplicación Google Authenticator** desde tiendas oficiales como Play Store o la App Store y haz clic en "Instalar".



2 Agrega un código.

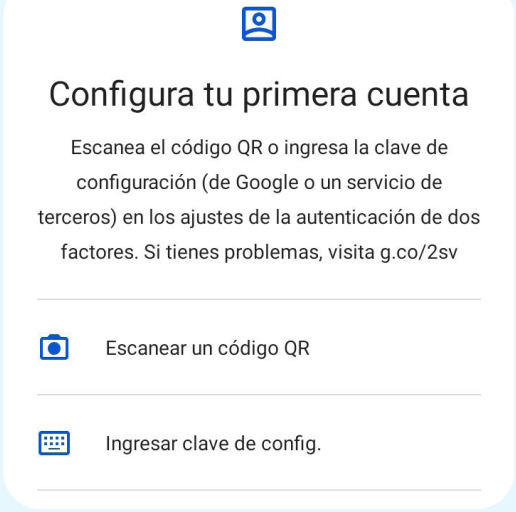
Google Authenticator te permite vincular tus cuentas de Google a la App para que sea más fácil recuperar tu información en caso de perdida o robo.

Si es tu primera vez usando la verificación en dos pasos la App te solicitará agregar un código para comenzar a proteger tus cuentas.

Deberás seleccionar la opción de "Agregar un código"

3 Configura tu primera cuenta.

Para comenzar a proteger tu información es necesario que registres las cuentas que deseas mantener seguras (Gmail, Facebook, Instagram, Twitter, etc.), para esto, deberás escanear el código QR de la cuenta que quieres proteger o en su defecto introducir una clave de configuración.



4 ¿Cómo obtengo un código QR?

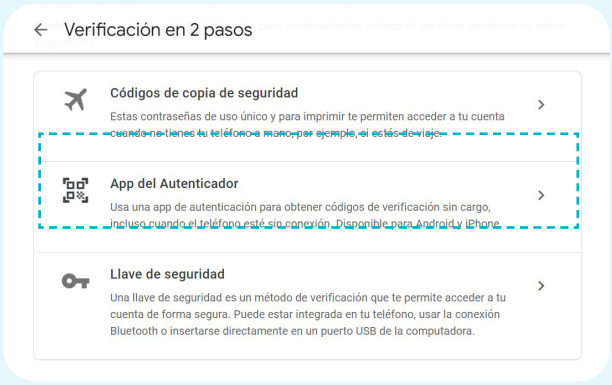
Los pasos a seguir para obtener un código QR varían dependiendo de cada cuenta, sin embargo podemos darte los pasos generales para obtenerlo.

- Abre tu **Cuenta.**
- En el panel de navegación, selecciona **Seguridad**.
- En la sección "Acceso", selecciona **Verificación en dos pasos-Comenzar.**
- Sigue los pasos que aparecen en pantalla.

Recuerda que es importante que abras tus cuentas en otro dispositivo, por ejemplo una computadora de confianza, esto para lograr escanear el código QR desde la app y lograr vincularla.

5 CONFIGURA LA APP DE AUTENTIFICACIÓN.

Una vez que localices el la opción de verificación en dos pasos dentro de la cuenta que deseas proteger, contarás con diferentes métodos de seguridad, es importante que selecciones la opción de “APP DEL AUTENTICADOR”.



Al seleccionar esta opción se abrirá una ventana que te mostrara el código QR que deberás escanear desde la App de Google authenticator.

6 ¿NO SE PUEDE ESCANEAR?

Si has seleccionado “Introducir clave de configuración”, haz clic en “¿No puedes escanearlo?”. A continuación, aparecerá una clave que deberás introducir en la aplicación junto con tu dirección de correo electrónico para finalizar la configuración.

7 HAS FINALIZADO LA CONFIGURACIÓN.

Una vez configurado el autenticador, la aplicación generará un código, que deberás introducir cada vez que quieras iniciar sesión en tu cuenta de Google desde un dispositivo nuevo

En el apartado (+) ubicado en la esquina inferior derecha podrás agregar las cuentas que quieras.

Si deseas conocer más a fondo sobre la verificación en dos pasos, cómo funciona y que beneficios tiene, puedes acceder a la sección de ayuda de Google en donde encontraras toda la información que necesites.

CENTRO DE AYUDA DE GOOGLE

https://support.google.com/accounts/answer/185839?hl=es-419&ref_topic=2954345&sjid=12035239743921861850-NA

¿QUIERES CONOCER UN POCO MÁS?

El Instituto Nacional de Ciberseguridad de España cuenta con diversas herramientas que podrán facilitar tu entendimiento, ingresa al siguiente link

https://www.youtube.com/watch?v=oFzKEogQEsI

¿Conoces los riesgos en línea que pueden afectar a tus estudiantes?

Es importante que los maestros conozcan los problemas online y offline de sus alumnos por varias razones:

IDENTIFICAR LAS NECESIDADES Y PREOCUPACIONES DE LOS ESTUDIANTES:

Al conocer las diferentes problemáticas que pueden enfrentar los estudiantes dentro y fuera de línea, los docentes pueden identificar sus necesidades y preocupaciones específicas, esto les permitirá adaptar su enfoque de enseñanza para satisfacer las necesidades individuales de las NNA.

FOMENTAR LA CONFIANZA Y LA COMUNICACIÓN ABIERTA:

Al conocer las problemáticas los maestros pueden fomentar la confianza y la comunicación abierta, los estudiantes se sentirán más cómodos compartiendo sus problemas y preocupaciones con un maestro que demuestra un interés genuino en su bienestar, lo que puede ayudar a crear una atmósfera positiva y de apoyo en el aula.

PROMOVER LA SEGURIDAD EN LÍNEA:

Los docentes pueden ayudar a los estudiantes a comprender los problemas digitales, como el acoso cibernético, el sexting y la privacidad en línea, al conocer los problemas digitales específicos que enfrentan los estudiantes, los maestros pueden ofrecer consejos y estrategias para mantenerse seguros en línea y evitar situaciones peligrosas.

Al estar informados sobre las necesidades y preocupaciones de los estudiantes, los docentes pueden proporcionar el apoyo y la orientación necesarios para ayudar a niñas, niños y adolescentes a alcanzar su máximo potencial y crecer como individuos.

Tipología de los riesgos en línea a los que se enfrentan NNA

Los peligros que enfrentan las NNA en Internet poseen diversos atributos, potenciales de daño y prevalencias, por lo cual resulta importante conocer cada uno de ellos.

	CONTENIDO **NNA como receptor** (de contenidos masivos)	**CONTACTO** **NNA como participante** (de actividades iniciadas por adultos)	**CONDUCTA** **NNA como actor** (perpetrador/víctima)
AGRESIVO	Contenidos violentos / de crueldad	Hostigamiento, acoso	Bullying, actividades hostiles entre pares
SEXUAL	Contenido pornográfico	Grooming, abuso sexual, encuentro con extraños	Acoso sexual, sexting
VALORES	Contenidos racistas o de odio	Persuasión ideológica	Contenido potencialmente dañino generado por el usuario

Si bien algunos riesgos digitales son dependientes de las nuevas tecnologías, otros surgieron mucho antes de su aparición y aprovechan las posibilidades que ofrece el medio a su favor, las mismas características de Internet que habilitan sus beneficios contribuyen a incrementar los potenciales riesgos.

2 DELITOS INFORMÁTICOS

Hablemos de delitos informáticos

Identifícalos para prevenir

Has llegado al capítulo II de esta Guía, aquí encontrarás los delitos informáticos más comunes que llegan a vulnerar a Niñas, Niños y Adolescentes, sus características, cómo actúan y algunas soluciones para atenderlos.

Sabemos que los docentes desempeñan un papel muy importante en la educación de las NNA, por ello, hablar sobre seguridad en línea, prevención de delitos informáticos y enseñar a los estudiantes a proteger su información personal ademas de utilizar Internet de manera segura es de vital importancia, ya que como docentes, figuras de autoridad y modelos a seguir, pueden desempeñar un papel importante en la prevención de estos delitos y comportamientos peligrosos en línea, así como dar una debida respuesta a estos delitos.

Es por lo anterior que queremos apoyarte en el proceso de prevención con tus estudiantes, esto para construir en conjunto un entorno online y offline más seguro para todas y todos.

¿Qué tanto conozco sobre los delitos informáticos?

Te presentamos una serie de afirmaciones que te ayudaran a medir tus conocimientos sobre los delitos informáticos, lee cuidadosamente cada afirmación y decide si la información es verdadera (V) o falsa (F).

No te preocupes si no conoces la respuesta a todas las afirmaciones, esta es una buena oportunidad para aprender y mejorar tu conocimiento sobre delitos informáticos para poder identificarlos.

	V	F
1.	La seguridad en línea no es importante, ya que los delincuentes informáticos sólo atacan a grandes empresas.	
2.	Los delitos informáticos sólo ocurren en computadoras, no en dispositivos móviles como teléfonos inteligentes o tabletas.	
3.	El phishing es un tipo de delito informático en el que se suplanta la identidad de una empresa o entidad para engañar al usuario y obtener información personal o financiera.	
4.	El acoso cibernético se refiere a comportamientos hostiles, intencionales y repetidos hacia una persona a través de dispositivos electrónicos.	
5.	La violencia digital se refiere a la utilización de tecnologías de la información y la comunicación (TIC) para difundir mensajes violentos, incitar a la violencia o amenazar a otras personas.	
6.	El grooming es una técnica utilizada por los depredadores sexuales para ganarse la confianza de los menores de edad en línea con el objetivo de realizar un encuentro sexual en persona.	
7.	La violencia digital puede incluir la publicación de fotos o vídeos privados sin el consentimiento de la persona involucrada.	
8.	El happy slapping es un tipo de violencia digital en el que se graba un ataque físico y se comparte en línea con fines de humillación.	
9.	El ciberacoso puede tener consecuencias graves para la salud mental de la víctima, como ansiedad, depresión y pensamientos suicidas.	
10.	Las madres, padres y cuidadores pueden ayudar a prevenir el acoso cibernético, el grooming y algún otro tipo de delito informático enseñando a las NNA sobre el uso seguro y responsable de la tecnología.	

Conoce las respuestas

1. La seguridad en línea no es importante, ya que los delincuentes informáticos sólo atacan a grandes empresas.

   FALSO

2. Los delitos informáticos sólo ocurren en computadoras, no en dispositivos móviles como teléfonos inteligentes o tabletas.

   FALSO

3. El phishing es un tipo de delito informático en el que se suplanta la identidad de una empresa o entidad para engañar al usuario y obtener información personal o financiera.

   VERDADERO

4. El acoso cibernético se refiere a comportamientos hostiles, intencionales y repetidos hacia una persona a través de dispositivos electrónicos.

   VERDADERO

5. La violencia digital se refiere a la utilización de tecnologías de la información y la comunicación (TIC) para difundir mensajes violentos, incitar a la violencia o amenazar a otras personas.

   VERDADERO

6. El grooming es una técnica utilizada por los depredadores sexuales para ganarse la confianza de los menores de edad en línea con el objetivo de realizar un encuentro sexual en persona.

   VERDADERO

7. La violencia digital puede incluir la publicación de fotos o vídeos privados sin el consentimiento de la persona involucrada.

   VERDADERO

8. El happy slapping es un tipo de violencia digital en el que se graba un ataque físico y se comparte en línea con fines de humillación.

   VERDADERO

9. El ciberacoso puede tener consecuencias graves para la salud mental de la víctima, como ansiedad, depresión y pensamientos suicidas.

   VERDADERO

10. Las madres, padres y cuidadores pueden ayudar a prevenir el acoso cibernético, el grooming y algún otro tipo de delito informático enseñando a las NNA sobre el uso seguro y responsable de la tecnología.

    VERDADERO

Conozcamos sobre Delitos Informáticos

¿Qué son los delitos informáticos?

Los delitos informáticos son aquellos actos ilegales que se cometen utilizando tecnologías de la información y la comunicación, como Internet, redes de computadoras, sistemas informáticos y dispositivos móviles, ya sea como medio o como un fin.

En resumen, los delitos informáticos son una forma de delincuencia que se comete en el ámbito digital, a través de la utilización de tecnologías de la información y la comunicación.

¿Medio y fin?, te presentamos dos ejemplos

MEDIO

Un programa de cómputo o cualquier otro dispositivo tecnológico será un medio para cometer un delito cuando es utilizado para obtener un beneficio, por ejemplo, acceder sin autorización a información confidencial. **La tecnología se convierte en la herramienta para delinquir.**

FIN

Un programa de cómputo o cualquier otro dispositivo tecnológico será el fin en un delito informático cuando recaiga sobre ese programa la conducta delictiva, como cuando se infecta de malware para destruir el programa. **Tu dispositivo se convierte en víctima.**

¿En dónde se encuentran tipificados?

En México, a partir de **1999,** la legislación penal federal tipifica ya algunas conductas como delitos informáticos. Sin embargo, algunas conductas delictivas que pudiesen ser consideradas como ciberdelitos siguen siendo consideradas como delitos tradicionales, por ello en los apartados siguientes te presentamos algunos artículos de diferentes Códigos y Leyes especiales que permiten salvaguardar la integridad de las NNA, ante amenazas en Internet.

¿Los identificas?

Te presentamos los delitos informáticos más comunes que vulneran a las NNA

1 Ciberbullying

CIBERACOSO O ACOSO CIBERNÉTICO

¿Qué es?

Víctimas de ciberacoso

29.3% 20.1%

Usuarios de 12 a 19 años (MOCIBA, 2022)

Es cuando una niña, niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otra persona de su misma edad a través de redes sociales y en general mediante Internet por medio de celulares, computadoras o tabletas, no es algo que ocurra una sola vez y se presenta de distintas formas, como insultos, discriminación o burlas.

¿En donde se encuentra tipificado?

Ley de Seguridad y Prevención Escolar de San Luis Potosí

Artículo 4° Para los efectos de esta ley, se entiende por:
I. Acoso escolar. "Conductas de diversa naturaleza como burlas, amenazas, intimidaciones, agresiones físicas y psicológicas, aislamiento sistemático e insultos, que tienden a originar problemas que se repiten y prolongan durante cierto tiempo dentro o fuera del establecimiento educativo, incluyendo los medios tecnológicos..."

¿Cómo se puede llegar a presentar el ciberbullying?

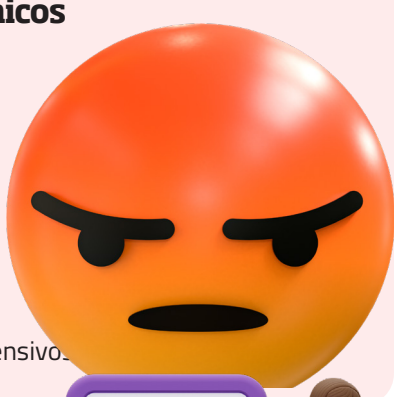
Conoce las diferentes formas:

Te presentamos algunos de los ejemplos sobre los diversos casos de ciberbullying en los últimos años, se debe recordar que el acoso cara a cara y el ciberacoso ocurren juntos a menudo, pero el ciberacoso deja una huella digital; es decir, un registro que puede servir de prueba para ayudar a detener el abuso.

Como docentes es importante que conozcas las diferentes formas en que se puede presentar el acoso cibernético para lograr atender la problemática.

Insultos electrónicos

Ofensas en las que algún usuario (a) hace a otro.



Ejemplo:
Creación de memes ofensivos.

Denigración

Se refiere a la difusión de información despectiva o falsa de alguna persona.

Ejemplo:
Publicación de fotografías alteradas.

Exclusión

Se realiza con la finalidad de excluir o no dejar participar.

Ejemplo:
Creación de grupos privados en alguna red social con la finalidad de burlase de alguien.

Suplantación

Implica que se hagan pasar por la víctima, ya sea utilizando sus contraseñas de acceso para enviar mensajes agresivos u ofensivos a terceras personas.

Ejemplo:
Creación de perfiles, secuestro de cuentas de WhatsApp, etc.

Extorsión/Doxeo

Radica en revelar información privada de la víctima que en un principio fue enviada por la víctima de forma privada para después difundirla a otras personas sin permiso de la víctima.

Ejemplo:
Amenazas por publicar información privada o de connotación sexual.

Hostigamiento

Implica el envío de mensajes ofensivos de forma reiterada a una persona determinada, ya sea por medio del correo electrónico, chats, mensajes de texto, etc.

Ejemplo:
Enviar o publicar mensajes, imágenes o videos abusivos o amenazantes.

Reportar contenido

Una respuesta inmediata

Es importante conocer los enlaces para reportar contenido en redes sociales porque nos permite actuar en contra de contenido inapropiado, ilegal o dañino que pueda estar circulando en las plataformas digitales. Estos enlaces nos brindan la oportunidad de informar a las autoridades o a los proveedores de servicios de las redes sociales sobre el contenido inapropiado que encontramos y así ayudar a prevenir la propagación de dicha actividad para proteger a otros usuarios.

Herramienta digital

Docente, **¿Necesitas reportar contenido de alguna red social o ayudar a tus estudiantes a hacerlo?,** te compartimos los enlaces de reporte para que puedan hacerlo de manera rápida.

Reportar una foto o un video de facebook que infringe mi privacidad.
https://es-la.Facebook.Com/help/contact/144059062408922

Reportar una foto o video que vulnere la intimidad de mi hijo/hija menor de 13 años.
https://es-la.Facebook.Com/help/contact/144059062408922

Reportar una foto o video que vulnere la intimidad de mi hijo/hija de entre 13 y 17 años.
https://es-la.Facebook.Com/help/contact/144059062408922

Reportar una foto o un video en facebook que vulnera la intimidad de una persona enferma, hospitalizada o con otra discapacidad.
https://es-la.Facebook.Com/help/contact/144059062408922

Reportar la cuenta de un nna menor de 13 años que usa la plataforma.
https://es-la.Facebook.Com/help/contact/209046679279097

Solicitud especial para eliminar la cuenta de una persona fallecida o con incapacidad médica.
https://es-la.Facebook.Com/help/contact/228813257197480

Denuncia la cuenta de un impostor
https://www.Facebook.Com/help/contact/295309487309948

Denunciar una cuenta comprometida
https://www.Facebook.Com/hacked

Reportar contenido en facebook que consideres difamatorio.
https://es-la.Facebook.Com/help/contact/430253071144967

Retirar información de google.
https://support.google.com/websearch/troubleshooter/3111061?hl=es

Retirar de google imágenes personales explícitas o íntimas no consentidas.
https://supoort.google.com/websearch/answer/6302812

Retirar pornografía falsa publicada sin consentimiento.
https://support.google.com/websearch/answer/9116649

Retirar de google contenido sobre mí de sitios en los que se llevan a cabo prácticas abusivas.
https://support.google.com/websearch/answer/9172218

Denunciar información privada de distintos tipos.
https://help.twitter.com/es/forms/safety-and-sensitive-content/private-information

Denunciar contenido en Instagram, como fotos o vídeos.
https://help.instagram.com/contact/383679321740945

Denunciar una infracción de derechos de autor.
https://help.instagram.com/contact/372592039493026

Denunciar contenido en TikTok.
https://www.tiktok.com/legal/report/feedback

Denunciar una cuenta de suplantación de identidad.
https://tiktokimpersonationusca.zendesk.com/hc/en-us/requests/new

2 Grooming

Cuando un adulto seduce a una NNA

¿Qué es?

El grooming online es el proceso por el cual un adulto, valiéndose de los medios que le ofrecen las tecnologías de la información y comunicación (TIC), entra en la dinámica de persuadir y victimizar sexualmente a NNA, tanto de manera física como a través de Internet, mediante la interacción y la obtención de material sexual de la víctima.

¿En donde se encuentra tipificado?

Código Penal Federal

Artículo 199 Septies

Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.

Código Penal de San Luis Potosí

Artículo 178 Bis

Comete el delito de abuso sexual equiparado, quien mediante el uso de medios electrónicos o de cualquier tecnología, contacte, obligue, induzca o facilite a una persona menor de dieciocho años, o de una persona que por su condición no tenga la capacidad de comprender el significado del hecho, o que no tiene capacidad para resistirlo, a realizar actos de exhibicionismo corporal o sexuales simulados o no, con fin lascivo o sexual.

¿Cómo se lleva a cabo el proceso de grooming?

Conoce las diferentes etapas

El grooming no inicia directamente pidiendo material sexual de algún tipo a las NNA, se lleva a cabo mediante etapas que permiten al agresor formar un vínculo completo de confianza para poder atacar completamente las vulnerabilidades de la víctima.

1 Acceso y contacto inicial

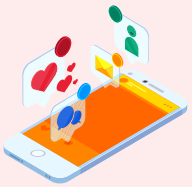
Este comienza con comportamientos encaminados a facilitar el inicio del contacto con las potenciales víctimas, los agresores suelen aprovechar diferentes escenarios desde los que puedan actuar.

Escenarios que facilitan el contacto inicial

Sitios de chat aleatorios.

Chats de un videojuego.

Redes sociales que no son privadas.



Grupos privados en redes sociales.

2 Estudio de la víctima y su entorno.

Una vez los adultos entablan una conversación con las NNA estudian a sus potenciales víctimas, con el objetivo de desarrollar estrategias más elaboradas y adaptadas a las respuestas que otorguen sus víctimas, buscando evaluarlos.

- Los agresores se interesan por conocer carencias familiares y materiales, estados de maltrato o negligencia.
- Se interesan por la vida diaria de las niñas, niños o adolescentes como horarios o actividades.
- Piden que no se comente a nadie sobre las conversaciones que se tienen.
- Hacen cumplidos a la víctima buscando mayor cercanía, algunos incluso "juegan a ser novios".

3 Estrategias de actuación.

Los agresores desarrollan una serie de estrategias de persuasión que parecen utilizar para adaptarse a las necesidades de las NNA.

4 Encuentros sexuales.

Con las estrategias desarrolladas los adultos consiguen su propósito de mantener relaciones sexuales con las NNA, tanto vía online (a través de intercambio de fotos o vídeos de contenido sexual) como offline (encuentros sexuales). Estos resultados son un contacto sexual puntual o un contacto sexual sostenido; asimismo, pueden haber sido realizados con una o múltiples víctimas.

3 Secuestro Virtual

¿Qué es?

Durante el 2022 a nivel nacional se registraron 5,056 delitos de extorsión por cada 100,000 habitantes en sus diferentes modalidades, siendo más afectados los hombres (ENVIPE, 2023).

El secuestro virtual, se inserta en una nueva modalidad de delincuencia "a distancia", en la que se emplean las tecnologías de la comunicación para realizar desde estafas, fraudes o extorsiones, en las que la víctima sufre un despojo, basado en el engaño para obtener su colaboración, la cooperación para el despojo se obtiene mediante la violencia verbal y psicológica que se ejerce a través de las amenazas a la integridad física o a la vida de un tercero relacionado afectivamente con la víctima.

¿En dónde se encuentra tipificado?

Código Penal Federal, (Extorsión).

Artículo 390

Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa.

Código Penal del Estado de San Luis Potosí, (Extorsión).

Artículo 230

Comete el delito de extorsión quien, para obtener un lucro para sí o para un tercero, intimide a otro con causarle un mal en su persona, familia o bienes, obligándolo a dar, hacer, dejar de hacer o tolerar algo. Este delito se sancionará con una pena de prisión de cuatro a diez años y sanción pecuniaria de cuatrocientos a mil días del valor de la unidad de medida y actualización.

- Cuando este delito se cometa utilizando cualquier medio de comunicación, a través de los que se pueda realizar la emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectué por hilos, radioelectricidad, medios ópticos, físicos, vía satelital, u otros sistemas electromagnéticos, o cualquier otro originado con motivo de los descubrimientos de la ciencia, se le impondrá de seis a doce años de prisión y sanción pecuniaria de seiscientos a mil doscientos días del valor de la unidad de medida y actualización.

¿Cómo se lleva a cabo el secuestro virtual?

Conoce las diferentes etapas

1. De manera aleatoria **los delincuentes se comunican esperando que alguien muerda el anzuelo y por medio de engaños e intimidación hacen que abandone su domicilio.**

2. Por lo general, el ciberdelincuente **argumenta ser integrantes de algún grupo delictivo; aseguran vigilar a la víctima y amenazan a la víctima con dañar a algún familiar si no sigue sus instrucciones.**

3. Para tener el control de la situación, **le solicitan trasladarse a algún sitio específico (hoteles, moteles, parques, restaurantes o algún lugar publico) y le exigen apagar su celular para limitar la comunicación con sus seres queridos o con las autoridades.**

4. Durante el tiempo en el que la víctima se encuentra incomunicada, **los extorsionadores llaman a los familiares argumentando un supuesto "secuestro" con el objetivo de conseguir lo más pronto posible el pago del "rescate".**

5. Los familiares al no poder mantener contacto con la persona que se encuentra "secuestrada" **realizan el pago del rescate mediante depósitos bancarios o transferencias en tiendas de conveniencia.**

4 Sexting

Enviar fotos o vídeos de contenido sexual

¿Qué es?

Etapa más vulnerable

33.6% **18.5**

Usuarios de 12 años o más (MOCIBA, 2022)

Existe una gran variedad de definiciones que aluden al término Sexting, que parte de las palabras en inglés "sex"/sexo y "texting"/envío de mensajes de texto a través de telefonía móvil, sin embargo, todas hacen referencia a la misma acción: enviar archivos multimedia con contenido de cierto nivel sexual tomadas o grabados por el protagonista de los mismos mediante el teléfono móvil.

¿En dónde se encuentra tipificado?

Código Penal Federal

Artículo 200

Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.

ATENCIÓN DOCENTE

Debemos recordar que el Sexting es una actividad consensuada que consiste en que voluntariamente la persona produce, publica, envía mensajes, fotos y vídeos con contenido sexualmente explícito de sí mismo.

¿Cuándo se configura como delito el Sexting?

Cuando se divulgan públicamente las fotos o vídeos con o sin el consentimiento del involucrado, se puede llegar a incurrir en delitos tales como: extorsión o difusión ilícita de imágenes.

¿Cuáles son los riesgos de llevar a cabo esta práctica?

1. El Sexting **supone la pérdida de la privacidad.**
2. La aparición de ciertos **comportamientos delictivos** como el grooming, el ciberbullying y la sextorsión.
3. En menor medida existe la posibilidad de que **la víctima llegue a ser acusado por producción de pornografía infantil.**

5 Sextorsión

Amenaza por hacer público contenido sexual personal

¿Qué es?

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) señala que la sextorsión supone el chantaje por parte de un ciberdelincuente para que la víctima realice una determinada acción o entregue una cantidad de dinero bajo la amenaza de publicar o compartir imágenes intimas que posee de la víctima.

La Ley Olimpia, considera "sextorsión" a la violencia digital que tiene como intensión "la acción dolosa de amenazar, chantajear, coaccionar o extorsionar a una mujer a exhibir contenidos sexuales sin consentimiento previo, por medio de las tecnologías de la información y la comunicación".

¿En dónde se encuentra tipificado?

Código Penal de San Luis Potosí

Artículo 187

Comete el delito de difusión ilícita de imágenes íntimas quien, transmita, publique, o difunda imágenes, sonidos o grabaciones de contenido sexual, que pueden o no contener texto, obtenidas con o sin el consentimiento de la víctima, sin autorización para su difusión. Este delito se sancionará con una pena de tres a seis años de prisión y multa de trescientos a seiscientos días del valor de la unidad de medida de actualización.

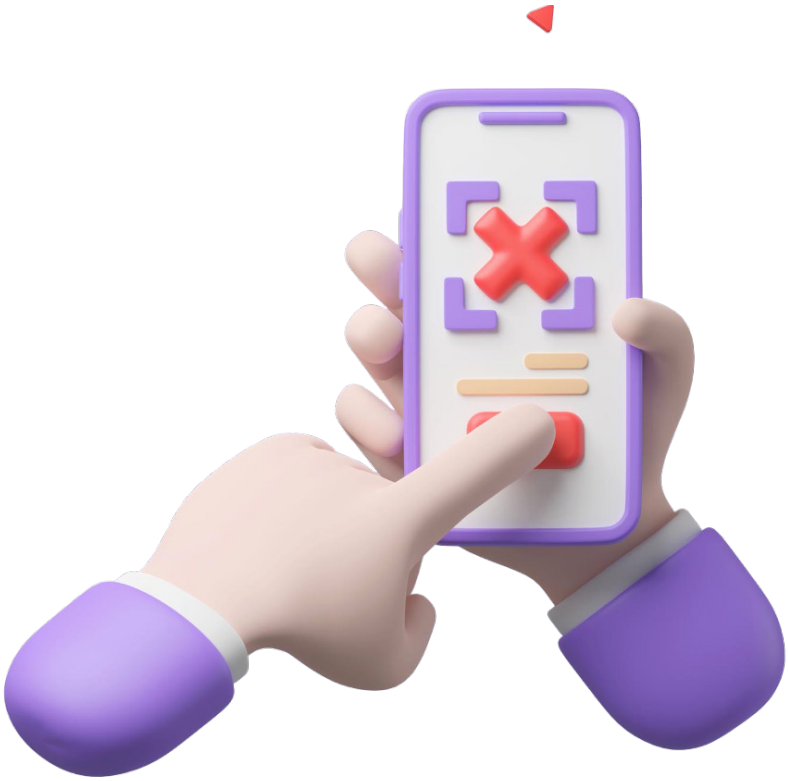
Código Penal del Estado de San Luis Potosí

Artículo 230

Comete el delito de extorsión quien, para obtener un lucro para sí o para un tercero, intimide a otro con causarle un mal en su persona, familia o bienes, obligándolo a dar, hacer, dejar de hacer o tolerar algo. Este delito se sancionará con una pena de prisión de cuatro a diez años y sanción pecuniaria de cuatrocientos a mil días del valor de la unidad de medida y actualización.

- Cuando este delito se cometa utilizando cualquier medio de comunicación, a través de los que se pueda realizar la emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectué por hilos, radioelectricidad, medios ópticos, físicos, vía satelital, u otros sistemas electromagnéticos, o cualquier otro originado con motivo de los descubrimientos de la ciencia, se le impondrá de seis a doce años de prisión y sanción pecuniaria de seiscientos a mil doscientos días del valor de la unidad de medida y actualización.

¿Cuáles son las condiciones necesarias para que se dé la sextorsión?



1

Una imagen íntima.

La imagen puede ser más o menos explícita o comprometedora, fotografía o vídeo, y su origen puede ser muy diverso como:

- Entregadas de forma voluntaria.
- Recibidas por terceras personas o encontradas de forma casual.
- Vulneradas o robadas por una intrusión en sistemas informáticos.
- Grabadas de forma consentida u oculta.

2

UN FIN POR OBTENER

Los tres fines habituales de la sextorsión son los siguientes:

- La satisfacción o dominio sexual.
- El Lucro: si la víctima debe aportar dinero u otro tipo de bien o servicio.
- El condicionamiento de conductas: donde la exigencia es hacer o dejar de hacer algo.

Herramienta digital

Docente, te presentamos **Nunca sin mi consentimiento,** la alternativa de facebook para evitar la sextorsión, un programa que permite ayudar a esas personas que se encuentran pasando por chantajes de personas que afirman tener contenido privado y que pueden publicarlo en las redes sociales si no se cumple con lo que piden.

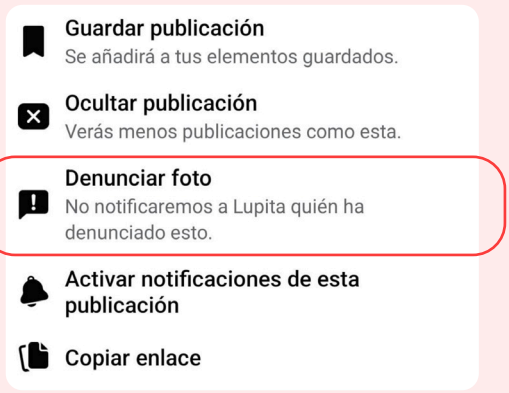
Informar a tus estudiantes sobre esta herramienta puede ayudarlos a evitar ser victimas, sin embargo, siempre recuerda que la **Policía Cibernética Municipal se encuentra a tu servicio.**

¿Cómo puedo reportar a Facebook una foto íntima mía que se compartió sin mi permiso?

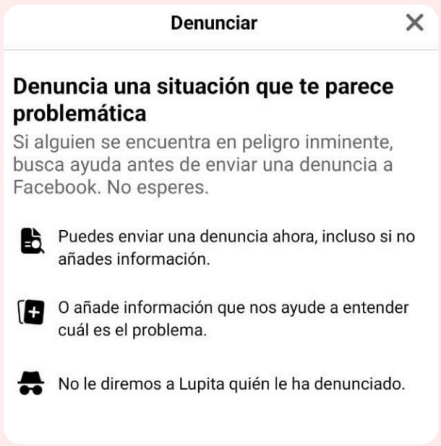
En Facebook, Instagram o Messenger, puedes denunciar que una persona haya compartido imágenes íntimas sin tu consentimiento o te haya amenazado con hacerlo.

1 **Haz clic en la foto o el video para expandirlos.** Si es un perfil restringido y no puedes ver la foto expandida, haz clic en **Buscar ayuda o reportar foto.**

2 **Haz clic en los tres puntos** ubicados en la parte derecha de la foto o el video.



3 Haz clic en **Reportar foto o Reportar video,** según corresponda.

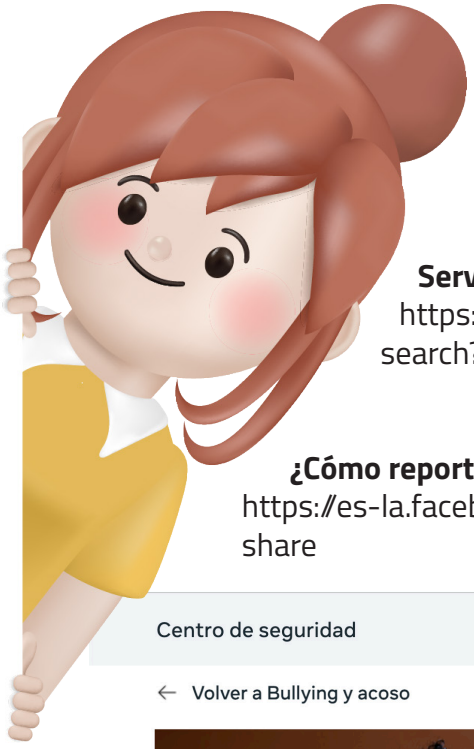


4 **Selecciona la opción** que mejor describa el problema y sigue las instrucciones que aparecen en pantalla.

Facebook usa tecnologías de comparación de fotos para impedir nuevos intentos de compartir la imagen en Facebook e Instagram. Si una persona intenta compartir la imagen después de que se reportó y eliminó, se le notificará que esto infringe las políticas de la red social y que se detuvo el intento de compartir la imagen. En la mayoría de los casos, también se inhabilitará la cuenta por compartir imágenes íntimas sin permiso.

¿Deseas conocer más?

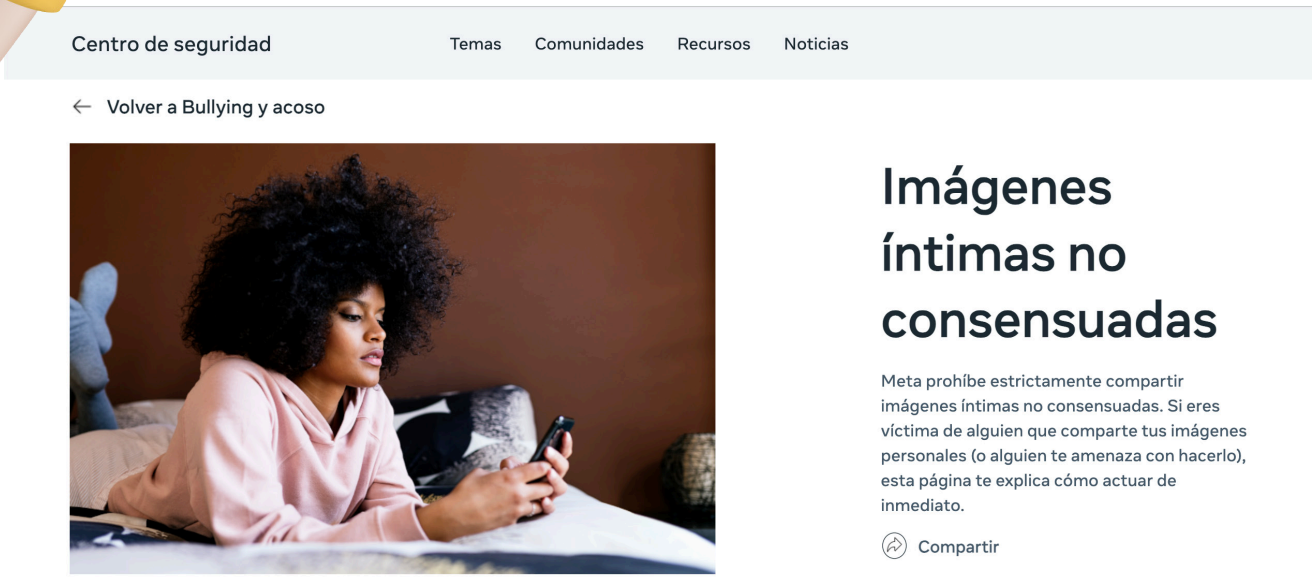
¡Echa un vistazo a los siguientes enlaces!



Página oficial de Facebook: "No sin mi consentimiento". https://es-es.facebook.com/safety/notwithoutmyconsent

Servicio de ayuda de Facebook: https://es-es.facebook.com/help/search?helpref=search&query=enlaces%20para%20reportar

¿Cómo reportar contenido en Facebook?: https://es-la.facebook.com/help/1432374603715654/?helpref=uf_share



6 Happy Slapping

BOFETADA FELIZ

¿Qué es?

El término happy slapping o bofetada feliz, en español, consiste en la **grabación de una agresión física, verbal o sexual y su difusión online mediante las tecnologías digitales en páginas, blogs, chats, redes sociales, entre otros,** lo común es que esta violencia se difunda por alguna red social, en ocasiones, logra hacerse viral, lo que puede llevar a muchas niñas, niños o adolescentes a sentirse vulnerables.

¿EN DÓNDE SE ENCUENTRA TIPIFICADO?

LEY DE SEGURIDAD Y PREVENCIÓN ESCOLAR DE SAN LUIS POTOSÍ

Artículo 4

Para los efectos de esta ley, se entiende por:

- **I. Acoso escolar.** "Conductas de diversa naturaleza como burlas, amenazas, intimidaciones, agresiones físicas y psicológicas, aislamiento sistemático e insultos, que tienden a originar problemas que se repiten y prolongan durante cierto tiempo dentro o fuera del establecimiento educativo, incluyendo los medios tecnológicos..."

LEY DE LOS DERECHOS DE NIÑOS, NIÑAS Y ADOLESCENTES DE SAN LUIS POTOSÍ .

Artículo 69.

Se considerará violación a su intimidad cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación locales, así como medios impresos, o en medios electrónicos de los que tenga control el concesionario o medio impreso del que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.

¿QUIÉNES PARTICIPAN EN ESTE ACTO VIOLENTO?

IDENTIFICA A LOS PARTICIPANTES (Save the Children, 2019)

Lo común es que el agresor físico y la persona que registra las imágenes tengan una intención previa de dar difusión al contenido grabado, esta violencia afecta aún más a la víctima sabiendo que la agresión se produce entre iguales.

En un 61% de los casos los agresores son amigas/amigos o compañeros, por esta razón, este tipo de agresión se relaciona directamente con el cyberbullying.

¿Cuáles son las fases del Happy Slapping?

CONOCE LAS DIFERENTES ETAPAS

1 ACUERDO PREVIO

Normalmente dos o más personas se ponen de acuerdo sobre cómo y cuándo poner en marcha una agresión física a otra compañera o compañero, la víctima suele ser una persona que ya sufre acoso o ciberacoso.

2 EL PRETEXTO

Los agresores suelen buscar una excusa para aislar a las NNA que van a ser acosadas. Prefieren zonas donde no puedan ser interrumpidos y donde no haya adultos que puedan parar la agresión.

3 LA AGRESIÓN FÍSICA

Cuando la víctima de happy slapping empieza a ser agredida suele haber una o más personas preparadas para grabar la escena y otros que golpean a la víctima. En otras ocasiones, se está produciendo la agresión y de forma espontánea, deciden grabarlo.

4 COMPARTIR LAS IMÁGENES

En el happy slapping, la agresión (que puede ser verbal, física o, en casos aún más graves, sexual) representa una primera fase, una vez terminada, la segunda fase consiste en la difusión de esta violencia en canales digitales.

7 Phishing

PESCA DE VÍCTIMAS

MÉXICO TIENE 85 MIL MILLONES DE INTENTOS DE CIBERATAQUE.
(CYBERSECURITY FORUM MÉXICO, 2022)

¿Qué es?

El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robar tu información privada, hacer algún cargo económico o infectar tu dispositivo, para lograrlo, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico.

¿Cuáles son los distintos tipos de estafa de phishing?

CONOCE CADA UNO

POR CORREO ELECTRÓNICO

Los mensajes de correo electrónico son, de largo, el **método más común para entregar el cebo del phishing.** Estos mensajes s contener enlaces que llevan hasta s web maliciosos o archivos adju infectados con malware.

POR SITIO WEB

Los sitios web de phishing, también conocidos como sitios falsificados, son **copias falsas de sitios web** que conoce y en los que confía. Los hackers crean estos sitios para engañarlo de modo que introduzcas tu usuario y contraseña, información que utilizarán para conectarse a tu cuentas.

SMISHING

Recibes un **mensaje de texto donde se te pide que hagas clic en un enlace o descargue una aplicación.** Sin embargo, al hacerlo te engañan para que descargues en tu teléfono un malware que puede captar tu información personal y enviarla al atacante.

VISHING

El atacante **intenta convencer por teléfono a las víctimas para que revelen información personal** que pueda utilizarse más adelante para el robo de identidad.

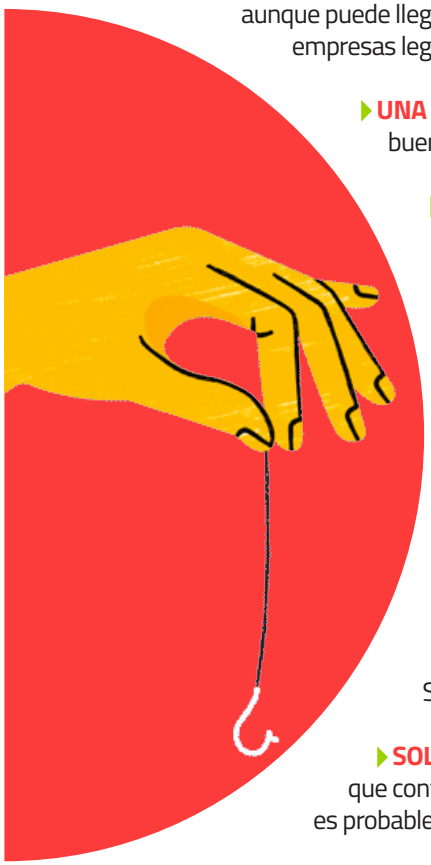
Herramienta digital

Docente, te presentamos **JIGSAW** una herramienta interactiva que te permitirá enseñar a tus estudiantes mediante un juego a identificar el aspecto que tiene un correo electrónico/mensaje/llamada de phishing.

La identificación de un ataque de ingeniería social de tipo phishing puede ser más difícil de lo que piensas, Jigsaw, la incubadora tecnológica de Google, lanzó una herramienta interactiva que pone aprueba la habilidad para identificar ataques de phishing por medio de un juego.

¿Podrías detectar qué es falso? **https://phishingquiz.withgoogle.com/?hl=es**

Identifica el aspecto que tiene un correo / llamada de phishing, toma en cuenta lo siguiente.



- **EL CORREO ELECTRÓNICO NO ESTÁ DIRIGIDO A TI.** Saluda de forma vaga, por ejemplo con «Estimado cliente», aunque puede llegar a utilizar tu nombre de usuario de correo electrónico. La correspondencia oficial de empresas legítimas se dirigirá a ti por tu nombre.
- **UNA OFERTA QUE NO PUEDES RECHAZAR.** Si te llega una oferta o ganga que parece demasiado buena para ser cierta, probablemente no sea cierta.
- **ARCHIVOS ADJUNTOS.** Aléjate de los archivos adjuntos desconocidos. Los estafadores pueden incluso ocultar un malware en archivos de contenido como los PDF.
- **ENLACES CON ERRORES.** Los hackers crean versiones falsificadas de sitios legítimos con URL que son casi idénticas, y te pueden animar en sus mensajes de phishing a hacer clic en estos enlaces. Debes estar atento a los errores deliberados, ya sean tipográficos u ortográficos.
- **FALTA EL CONTENIDO DE FIRMA.** Falta el contenido de firma típico que cabría esperar de un correo electrónico oficial.
- **ENLACES ACORTADOS.** Se doblemente suspicaz con los enlaces cuando consultes el correo electrónico con tu teléfono.
- **TÚ NO UTILIZAS ESA EMPRESA O SERVICIO.** Si recibes un mensaje de Servicios de Streaming A, pero tú eres un fiel cliente de Servicios de Streaming B o C, se trata de phishing.
- **SOLICITUDES DE INFORMACIÓN PERSONAL.** Si recibes un correo electrónico donde te piden que confirmes tu información de cuenta, las credenciales de inicio de sesión u otros datos personales, es probable que se trate de una estafa.
- **MENSAJES ESCRITOS DE FORMA INCORRECTA.** El banco no envía correos electrónicos llenos de faltas de ortografía y errores gramaticales. Un phisher sí que puede, y a menudo lo hace.
- **DEBES ACTUAR DE INMEDIATO.** Ninguna entidad legítima, ni gubernamental, ni empresarial ni de ninguna clase, te dará una única y urgentísima posibilidad antes de cerrarte la puerta.

8 Violencia Online

En la pareja o ex pareja

¿Qué es?

ETAPA MÁS VULNERABLE

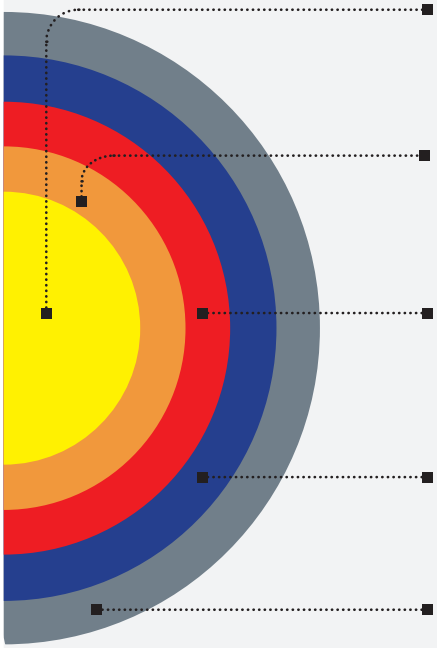
PAREJA 0.6 6.1% **EX PAREJA**

USUARIOS DE 12 AÑOS O MÁS (MOCIBA, 2022)

Esta violencia se define como el conjunto de comportamientos repetidos que pretenden controlar, menoscabar o causar daño a la pareja o ex pareja, es muy probable que quien sufra o provoque violencia en el mundo físico lo haga también en el virtual, se suele llevar a cabo mediante mensajes, control de las redes sociales, apropiación de las contraseñas, difusión de secretos o información comprometida, amenazas e insultos.

CONOCE LOS INDICADORES

Como docente puedes llegar a identificar situaciones entre tus estudiantes que culminen en algún tipo de violencia, por ello conocer los indicadores es muy importante.



- Acosar o controlar a la pareja mediante el teléfono móvil.
- Espiar el móvil de la pareja y/o acusar de falta de confianza o de que hay algo que ocultar si no se permite.
- Enfadarse por no recibir respuesta inmediata en redes sociales y/o aplicaciones como WhatsApp.
- Obligar a que la pareja muestre las conversaciones personales con otras personas.
- Censurar y obligar a retirar fotografías de la pareja en redes sociales.
- Controlar a quién se sigue, a quién se comenta, quién sigue a la pareja y los comentarios que se puedan cruzar, así como los likes, etc.
- Exigir la geolocalización para tener controlada a la pareja las 24 horas del día.
- Comprometer a la pareja para que se compartan contraseñas de cuentas personales.
- Obligar a la pareja a que envíe imágenes íntimas, ya sea mediante amenazas o chantaje emocional.

9 Otras situaciones que pueden resultar riesgosas y que se deben considerar

Incitación a conductas dañinas.

Las NNA pueden verse realmente afectados por ciertos contenidos que descubren a través de internet, esta exposición puede afectar su salud e integridad física, ya que existen plataformas que promocionan comportamientos como la autolesión o los trastornos alimenticios, dando consejos sobre cómo llevarlos a cabo.

Como docente, es importante estar consciente de que los retos virales o conductas dañinas en línea pueden tener un impacto negativo en la seguridad y el bienestar de los estudiantes, por lo tanto, es crucial tomar las medidas para abordar este problema y educar a NNA sobre los riesgos asociados con estas prácticas.

Supervisar el uso de dispositivos y redes sociales: Supervisar el uso de dispositivos y redes sociales en el aula y establecer reglas claras para el uso responsable de la tecnología es un buen comienzo.

Conocer los retos virales actuales: Mantenerse informado sobre los retos virales actuales y estar preparado para abordar cualquier situación que pueda surgir en el aula.

Exposición involuntaria a material sexual y/o violento.

Al referirnos a la exposición involuntaria a material sexual y/o violento, hablamos de la exposición a imágenes, video, audios, textos de índole sexual mientras una persona realiza una búsqueda online, navega por la red o abre su correo electrónico, siempre y cuando no busque voluntariamente ni espere ver material sexual.

Es importante estar preparado para abordar la exposición de material sexual o violento que los estudiantes reciben por Internet y tomar medidas para proteger y apoyar a las NNA afectados, al ofrecer un ambiente seguro, confidencial y brindar educación así como apoyo emocional, esto puede ayudar a los estudiantes a superar estas experiencias y mantenerse seguros en línea.

10 ¿Tus estudiantes frecuentan estas páginas?

Mantente alerta

Páginas *Gore* y de *Narcocultura*

¿Qué son?

Las páginas de contenido gore y narcocultura son sitios en la red que muestran la incorporación del narcomundo y sus actividades de manera explícita, generando expectativas de vida por medio de representaciones positivas e imaginarias sobre el narcotráfico, creando en la población más joven aspiraciones y anhelos sobre el narcomundo, además de la normalización de conductas delictivas.

Contenido Narco

Expone al narcotráfico como una **actividad ilegal y a la vez como una forma de vida** que se legitima y que resulta en el engrandecimiento y poder de las personas que lo ejercen.

Contenido Gore

Contenido que se centra deliberadamente en **representaciones gráficas de sangre y violencia.**

¿Qué puede ocurrir cuando nos exponemos a este contenido?

La exposición a estas páginas o sitios de Internet pueden generar un sentido de normalidad y aceptación a conductas poco favorables para niñas, niños y adolescentes, sin mencionar que muchas de estas páginas tienen como propósito atraerlos para unirse a las filas del crimen en los puestos más bajos y peligros de la organización o atrapar a nuevos clientes.

Páginas de *Flaming* y comunidades tóxicas

¿Qué es?

Flaming se define como el acto de publicar o enviar mensajes ofensivos a través de Internet, estos mensajes se denominan «llamas» y pueden publicarse en foros de discusión en línea o grupos de noticias, también pueden enviarse por correo electrónico o programas de mensajería instantánea. El lugar más común donde se produce el flaming son los foros de discusión online.

¿Qué causa?

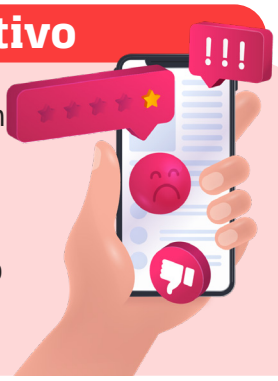
Ser víctima de flaming puede ocasionar daños a la reputación, disminución de la confianza y el autoestima, sin embargo, la exposición constante a páginas nocivas que promueven este tipo de prácticas crean un entorno digital nocivo que puede traspasar al mundo físico, por lo que fomentar el respeto dentro y fuera de Internet es prioridad.

Tipos de flaming

En el flaming el ataque es lanzado o provocado, con la finalidad de que alguien "pique" y entre en su juego.

Flaming corporativo

Consiste en enviar una gran cantidad de comentarios críticos, generalmente agresivos o insultantes, a los empleados, productos o marcas de una empresa.



Pie fights

Una pelea de tartas (Pie Fight) se caracteriza por argumentaciones encendidas y enormemente emocionales sobre un tema delicado que no tiene nada que ver con el tema habitual del foro en cuestión.

Flame wars

Una guerra de fuego tiene lugar cuando varios usuarios se involucran en respuestas provocativas a una publicación original, que muchas veces es un cebo, atraen a muchos usuarios, incluidos aquellos que intentan desactivar la guerra de llamas y pueden convertirse rápidamente en una guerra de llamas masiva en donde todos insultan a todos.

Plataformas +18 como OnlyFans

¿Qué es?

OnlyFans es una plataforma de suscripción por contenido exclusivo, en ella existen perfiles similares a los de otras redes sociales como Facebook, Twitter o Instagram, pero con la diferencia en la que es necesario pagar una suscripción para seguir y ver el contenido de alguien, sin embargo también existen las suscripciones gratuitas de creadores de contenido que muestran su material sin tener que pagar por ello.

¿Qué contenido se puede encontrar en onlyfans?

OnlyFans es una plataforma que se ha encaminado a ofrecer contenido para adultos, donde se explota el tema erótico o contenido con insinuaciones sexuales; sin embargo, en OnlyFans hay otro tipo de creadores de contenido, como entrenadores de gimnasio, artistas, nutriólogos y demás personas que venden sus conocimientos por medio de imágenes o vídeos a cambio de una suscripción.

18+

PARA CREAR UNA CUENTA

Es requisito contar con más de 18 años de edad y aceptar los términos y condiciones de la plataforma; además, solicitan información personal con la finalidad de dar certidumbre a los perfiles y evitar posibles fraudes.

Lo anterior puede hacernos pensar que es una plataforma únicamente para adultos, sin embargo, el contenido que se encuentra puede ser filtrado al acceso público, lo que termina por exponer a personas fuera del rango de edad solicitado.

Se debe tener en cuenta que las fotos, videos o mensajes que se suben a la plataforma pueden ser filtrados, publicados o distribuidos en especial si se elige onlyfans gratis, aumentando el riesgo de acoso e intentos de extorsión.

Plataformas sociales como Reddit, 4chan o Discord

¿Qué son ?

Son plataformas para que personas con intereses similares compartan y se comuniquen, estas plataformas son populares entre diversas comunidades con intereses distintos.

¿Son plataformas seguras?

Las plataformas están diseñadas para ser usada por adultos, no es conveniente que las NNA se registren y utilicen estas comunidades, puesto que pueden ser susceptibles a fugas de información o ser victimas de depredadores.

Querrás considerar la madurez de las NNA, ¿cómo respondería la NNA si encuentra contenido para adultos? incluso existiendo moderadores de seguridad, la probabilidad de que un NNA se tope con algo inapropiado es alta.

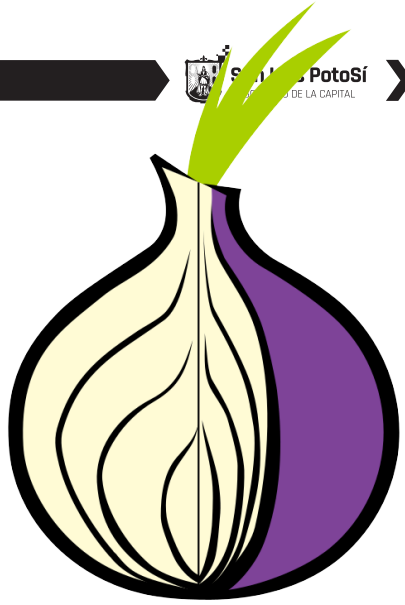
¿Cuáles son los riesgos de usar estas plataformas?

La mayoría del contenido de estas plataformas está creado por adultos, debido a ello, hay muchos riesgos para las niñas, niños y adolescentes.

- Grupos de chat con desconocidos
- Retos peligrosos o inapropiados
- Depredadores
- Fuga de información personal
- Desinformación
- Contenido inapropiado

No es necesario ser un miembro registrado para leer contenido, cualquiera puede acceder al contenido de la web, una vez te registras, podrás visualizar un feed con las entradas que son tendencia y debajo de ellas las publicaciones más populares basadas en tu configuración (ubicación, intereses y privacidad).

Navegadores de internet como Tor Browser, 12P, Whonix-Workstation



¿Qué son?

Son aplicaciones de navegación en Internet creadas para cualquier usuario que busque mantenerse anónimo y obtener seguridad extra en línea, están diseñadas para detener el acceso a tus registros en linea como el modo en el que navegas.

¿Es seguro su uso?

Si bien, estos navegadores ayudan a proteger la anonimidad del usuario, su uso por parte de NNA puede ser un riesgo.

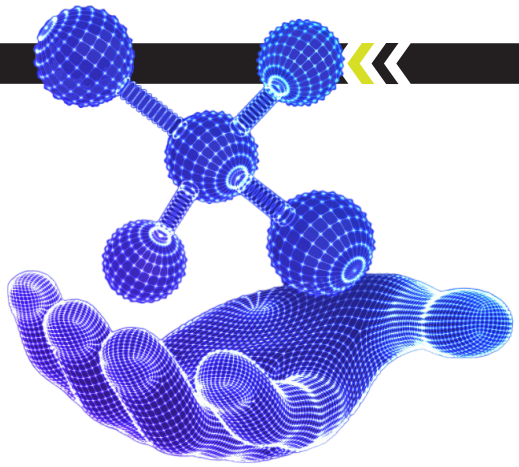
El emplear una red TOR permite ingresar a la darknet (red oscura); paginas web y servicios que no se encuentran de forma ordinaria (indexada) como en Google, por lo que es el cobijo de muchos delincuentes.

¿Cuáles son los riesgos de usar estos navegadores?

Estos navegadores exponen a las desventajas de la darknet, en donde se pueden encontrar actividades ilegales, tales como la venta de datos sensibles, pornografía infantil, venta de estupefacientes entre otros. El uso de estos navegadores los puede llevar a encuentros directos con actores maliciosos.

Deepnude

Aplicación que "desnuda" a cualquier mujer mediante inteligencia artificial



¿Qué es?

Es una aplicación que utiliza IA (inteligencia artificial) y redes neuronales para eliminar la ropa de imágenes de mujeres y recrear desnudos ultra realistas.

Se trata de una evolución de los llamados Deep Fakes, un nuevo algoritmo que nos anticipa el gran potencial que tiene esta tecnología y sus impacto sociales.

¿Sólo recrea imágenes de mujeres?

La aplicación consigue crear desnudos en segundos, dejando en manos de cualquier persona poder generar una imagen así.

Es importante decir que el algoritmo únicamente funciona con mujeres, ya que cuando se aplica en una imagen de un hombre en lugar de mostrar partes masculinas, añade órganos femeninos de manera instantánea.

¿Cuáles son los principales problemas?

Personas han sido victimas de "sextorsión" mediante vídeos e imágenes suyas manipuladas por Inteligencia Artificial para la creación de material sexual falso, los cibercriminales divulgan este material en redes sociales o sitios de pornografía para extorsionar a las víctimas.

Las imágenes y vídeos se pueden obtener directamente de las redes sociales, fuentes públicas o incluso pueden ser directamente proporcionadas por la víctima.

¿Qué podemos hacer?

- **Configura tu privacidad en redes sociales y aplicaciones, no aceptes a desconocidos.**
- **No respondas los mensajes, reporta, bloquea y denuncia.**
- **Contacta de manera inmediata con las autoridades.**

Páginas de compra y venta
fraudes en compra por internet

¿Qué son ?

Son páginas en donde se lleva a cabo la compra y venta de productos o servicios de forma digital, esta actividad comercial puede darse a través de sitios web, redes sociales o plataformas de comercio en línea.

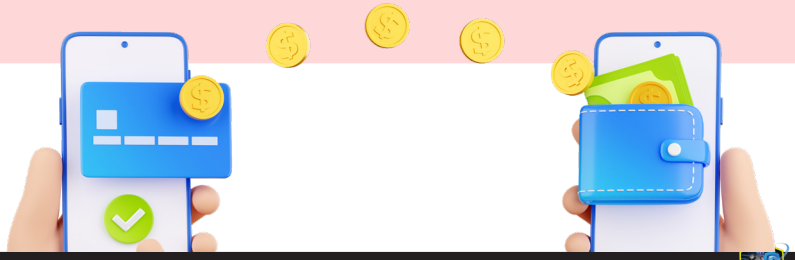
¿Es seguro su uso?

El desconocimiento de las TIC de muchos usuarios provoca que éstos cometan errores a la hora de realizar compras online y terminen siendo víctimas de algún fraude, para las NNA el riesgo puede ser mayor al dejarse llevar por el producto y no atender las señales que pueden alertar sobre un posible fraude.

Señales para no comprar en Internet

No necesitas renunciar a la facilidad y la selección interminable de compras por internet, pero estas precauciones pueden ayudar a asegurarte de obtener lo que pagas.

- **Muestren precios extremadamente bajos, alejados de los precios reales o todo cuesta lo mismo.**
- **Nos piden los datos personales y financieros para realizar el pago, en páginas sin certificado digital.**
- **No suelen usar paginas de pago como Pay Pal, por el contrario, prefieren transferencias a través de tiendas de conveniencia.**
- **Los datos de la empresa como ubicación o nombre legal no están disponibles o bien no se puede comprobar su autenticidad.**



Actuación Docente

Si un docente detecta un caso de delito informático en su escuela, es importante que tome medidas inmediatas para proteger a sus estudiantes, prevenir futuros incidentes y denunciar el percance a la Policía Cibernética Municipal

Algunas acciones que puede realizar el docente en este caso son:

1

Notificar a la dirección de la escuela:

El docente debe informar de inmediato a la dirección de la escuela sobre el incidente de delito informático y proporcionar toda la información disponible, por lo que se debe recopilar información para entender cómo sucedió y quiénes fueron los responsables, teniendo siempre en cuenta la no revictimización del afectado.

2

Proteger a los estudiantes afectados:

Si un estudiante ha sido víctima de delito informático, el docente debe tomar medidas inmediatas para protegerlo, como contactar a los padres, derivarlo a un servicio de salud mental o brindar apoyo emocional.

3

Comunicar a las madres, padres o cuidadores:

El docente debe informar a las madres. padres o cuidadores sobre el incidente de delito informático y trabajar en conjunto para prevenir futuros casos y brindar todo el apoyo posible.

4

Recopilar pruebas:

Con autorización de la NNA afectado y siempre explicándole la necesidad de guardar la información del hecho, el docente debe auxiliar a recopilar todas las pruebas posibles del delito informático, como capturas de pantalla o grabaciones de video, para ayudar a la investigación, en caso posible la madre, padre o tutor deberá realizar esta acción.

5

Buscar apoyo y denunciar el incidente a las autoridades:

La institución educativa debe buscar ayuda de las autoridades competentes, la Policía Cibernética del Municipio de San Luis Potosí, cuenta con diferentes canales de comunicación a los que se podrán comunicar en busca de guía y apoyo, de igual manera, pueden auxiliar en el proceso de denuncia como primer respondiente dando seguimiento a todo el proceso correspondiente para garantizar que se protejan los derechos de los estudiantes.

6

Aplicar medidas disciplinarias:

Si un estudiante ha sido el autor del hecho, es importante ayudarlo a entender la afectación que ha provocado el hecho y hablar sobre el motivo de su accionar, de igual manera se deberá aplicar alguna sanciones según lo establecido en el reglamento interno de la escuela.

Comunicación con Niñas, Niños y Adolescentes en riesgo

Hablar con niñas, niños o adolescentes que son víctimas de delitos informáticos o violencia digital puede ser una tarea delicada y un proceso difícil, como docente, es importante ser comprensivo y estar disponible para ayudar al niño en todo lo que necesite.

Aquí hay algunos consejos que pueden ser útiles:

Escuchar activamente:

Es importante que la niña, niño o adolescente se sienta escuchado y comprendido, escucha activamente sus preocupaciones y hazle saber que su bienestar es prioridad.

Validar sus sentimientos:

Hazle saber a la NNA que sus sentimientos son válidos y que no está solo, pregúntale cómo se siente y asegúrate de que se sienta comprendido.

Proporcionar apoyo emocional:

Brinda apoyo emocional y refuerza la idea de que no es culpa suya lo que ha ocurrido.

Da información:

Es inherente que el NNA entienda lo que ha sucedido y por qué es importante informar sobre lo que ha sucedido.

Proporcionar recursos:

Proporciona información sobre recursos y apoyo profesional para ayudar al NNA a superar lo que ha ocurrido.

Tomar medidas:

Es imprescindible tomar medidas para proteger a la NNA y prevenir futuros delitos informáticos.

Involucra a madres, padres y cuidadores:

Es vital involucrar a estas figuras en el proceso y trabajar juntos para abordar el problema y proporcionarles la información necesaria para ayudar al NNA.

Comunicación con Niñas, Niños y Adolescentes con conductas antisociales en el mundo digital

Aquellas NNA que llevan a cabo conductas antisociales en el mundo digital y que afectan a otros o a sí mismo, involucra que seamos comprensivos y estar disponible para ayudar a la NNA a que comprendan el impacto de sus acciones con la finalidad de tomar medidas para prevenir futuros incidentes informáticos.

Te presentamos algunos consejos que pueden ser útiles:

Siempre escucha:

Antes de juzgar, es importante escuchar la versión de la niña, niño o adolescente, asegúrate de escuchar activamente lo que la NNA tiene que decir sin interrumpir o juzgar.

Explicar las consecuencias:

Es importante que la NNA comprenda las consecuencias de sus acciones, explícale las implicaciones de sus acciones y cómo pueden afectar a otras personas o a sí mismos.

Enseñar el impacto:

Hazle saber a la NNA que sus acciones pueden lastimar a otros y dañar su reputación y las relaciones que tiene con otras personas.

Involucra a madres, padres y cuidadores:

Es importante involucrar a estas figuras en el proceso y trabajar juntos para abordar el problema, proporcionarles la información necesaria para ayudar a la NNA a entender el impacto de sus acciones y prevenir futuros delitos informáticos.

Proporcionar recursos:

Proporciona a la niña, niño o adolescente recursos y apoyo profesional para ayudarlo a superar sus comportamientos dañinos.

Tomar medidas:

Es importante tomar medidas apropiadas para abordar el comportamiento de la niña, niño o adolescente y prevenir futuros delitos informáticos, siempre procurando el apoyo sano y sin prejuicios.

Comunicación con madres, padres y cuidadores

Si un docente detecta un incidente informático que involucra a un estudiante, es importante que se comunique de manera inmediata y clara con la madre, padre o cuidador del estudiante involucrado.

Algunas sugerencias para abordar esta situación de manera efectiva pueden incluir:

1

Programar una reunión con la madre, padre o cuidador del estudiante involucrado:

Es vital que el docente establezca una reunión con las madres, padres o tutores del estudiante lo antes posible para discutir el incidente informático y las acciones que se están tomando para abordar la situación. Es importante que sea claro y honesto sobre la situación y proporcione detalles específicos sobre lo que se está haciendo para investigar el incidente.

2

Proporcionar recursos y apoyo:

Es fundamental que el docente brinde a la madre, padre o cuidador recursos y apoyo para abordar la situación con el estudiante, esto puede incluir proporcionar información sobre cómo hablar con las NNA sobre los peligros en línea, brindar información sobre instituciones especializadas en ese tipo de problemáticas o referirlos a un profesional de la salud mental.

3

Tomar medidas para garantizar la seguridad del estudiante:

Si el incidente informático ha puesto al estudiante en peligro, es importante que el docente tome medidas para garantizar su seguridad. Esto puede incluir trabajar con las autoridades locales para presentar una denuncia y garantizar que se tomen medidas para proteger al estudiante de cualquier amenaza.

4

Mantener la comunicación:

Después de la reunión inicial, merece la atención que el docente mantenga una comunicación abierta y regular con la madre, padre o cuidador del estudiante para asegurarse de que se están tomando medidas adecuadas para abordar la situación. También debe de seguir trabajando en equipo para garantizar que el estudiante tenga el apoyo y la ayuda que necesita para superar cualquier trauma o impacto emocional que pueda haber experimentado como resultado del delito informático.

Recomendaciones para hablar con cualquier tipo de madre, padre o cuidador

Hablar con tantas madres, padres o cuidadores puede ser un desafío para cualquier docente, en el caso de hablar sobre alguna problemática de tipo informático puede serlo aun más, en general, es importante recordar que el objetivo principal es resolver el problema y mantener una comunicación efectiva y respetuosa, incluso si eso significa establecer límites claros en algunas situaciones.

A continuación se presentan algunas estrategias que pueden ayudar a manejar estas situaciones:

1. **Mantener la calma:**
Es importante mantener la calma y la profesionalidad en todo momento, incluso si la madre, padre o cuidador está siendo argumentativo.

2. **Escuchar activamente:**
Permitir que la madre, padre o cuidador expresen sus preocupaciones sin interrupciones y escuchar activamente lo que están diciendo.

3. **Mostrar empatía:**
Tratar de entender los sentimientos de la madre, padre o cuidador y expresar empatía por su situación.

4. **Ser claro y directo:**
Explicar claramente la situación y la perspectiva de la escuela o el docente sobre el problema.

5. **Proporcionar soluciones:**
Ofrecer soluciones prácticas y sugerencias para resolver el problema.

6. **Establecer límites:**
Si la madre, padre o cuidador esta siendo muy efusivo o abusivo, es importante establecer límites claros y directos sobre lo que es aceptable y lo que no es aceptable en las interacciones.

7. **Buscar ayuda:**
Si el problema persiste o se intensifica, buscar la ayuda de un supervisor o un consejero escolar puede ser útil.

Conoce a tus aliados

Es crucial que los docentes conozcan a las autoridades a las que pueden acudir en caso de detectar un incidente informático en su escuela, esto les permitirá tomar medidas adecuadas para proteger a los estudiantes.

Policía Cibernética de la Secretaría de Seguridad y Protección Ciudadana del Municipio de San Luis Potosí

La Policía Cibernética Municipal es una Jefatura que cuenta con personal especializado y altamente capacitado en incidentes de tipo informático.

¿Cómo pueden ayudarme?

Prevención de delitos:
La Policía Cibernética Municipal trabaja en la prevención de delitos informáticos mediante la identificación de posibles amenazas, visibilizando acciones en ciberseguridad para su protección.

Protección de víctimas:
La Policía Cibernética Municipal puede proporcionar asesoramiento y apoyo a las víctimas de delitos informáticos, recabar indicios y/o evidencias, así como tomar medidas de contención, protección y cuidado ante un ciberataque.

Asesoría:
La Policía Cibernética Municipal puede proporcionar asesoría sobre algún incidente en ciberseguridad y brindarte información sobre las mejores acciones de protección.

Investigación de delitos:
La Policía Cibernética Municipal tiene experiencia y capacitación especializada para investigar delitos informáticos, lo que les permite recopilar y analizar pruebas digitales para identificar a los responsables, mediante la actuación fehaciente y legal, por medio de inteligencia de fuentes abiertas, así como colaboración con las diferentes agencias del orden.

¿En dónde puedo contactarlos?

¿Buscas asesoría de manera personal?, visítanos:
Calle 6ª. Oriente No. 455, Col. Central de Abastos, San Luis Potosí, S.L.P

¿Deseas una atención telefónica o por WhatsApp? Comunícate:
444-329-32-81

¿Prefieres usar facebook?, mándanos mensaje:
Policía Cibernética Municipal SSPC SLP.
https://www.facebook.com/Ciber.SSPC

¿Instagram es tu app favorita?, también estamos ahí:
Ciber.sspcslp.
https://instagram.com/ciber.sspcslp?igshid=Yzg5MTU1MDY=

¿Quizás prefieres una atención por Twitter?, adelante:
@Ciber_SSPCSLP
https://twitter.com/Ciber_SSPCSLP

Estamos en todos lados, contáctanos en telegram:
444-329-32-81

También puedes contactarnos por correo:
policiacibernetica@sanluis.gob.mx

No estaría mal que nos contactaras también por Tik Tok:
ciber.sspcslp
https://www.tiktok.com/@ciber.sspcslp?is_from_webapp=1&sender_device=pc

Siempre es importante conocer

¿Cómo se lleva a cabo el proceso de denuncia?

1 Localiza dónde denunciar

Para realizar una denuncia puedes hacerlo de tres maneras:

- Acudiendo personalmente ante la Fiscalía del Estado o Fiscalía General de la República.
  - **FGE:** Eje Vial Ponciano Arriaga 100, Zona Centro, 78000 San Luis, S.L.P.
  - **FGR:** Polonia 370, Lomas de Satelite, 78384 San Luis, S.L.P.
- De manera virtual en la página oficial de la Fiscalía del Estado, https://fiscaliaslp.gob.mx/vi/denuncia_virtual/
- Por medio del acompañamiento de nuestros Analistas Especializados, acudiendo a nuestro módulo de atención.

2 ¿Qué necesitamos?

- Documentación oficial de identidad vigente, con copia, ya sea tu cédula profesional, credencial para votar, licencia de conducir, pasaporte, entre otros.
- Un correo electrónico activo para contactar con las autoridades.
- Tener un recuento de los hechos lo más detallado posible y evidencias si cuentas con ellas.

3 ¿Cómo se inicia el proceso?

1. Dirígete a las autoridades correspondientes y relata cómo sucedió el delito, deberás brindar todos los detalles: lugar y hora, si hubo testigos, descripción de quién cometió el delito y si existen antecedentes de amenazas o agresiones con esta misma persona.
2. En caso de requerirse, te pedirán que te realicen exámenes médicos y psicológicos, pero tranquilo, este tipo de servicios los puedes obtener de manera gratuita por parte de la institución.
3. Puedes solicitar medidas especiales si lo necesitas (por razones de género, discapacidad o por pertenecer a un pueblo o comunidad indígena), la autoridad debe garantizar que tengas acceso a ellas para que puedas denunciar.
4. Recuerda que las autoridades deben cumplir con sus obligaciones, no pueden pedirte dinero o rehusarse a hacer su trabajo; si sufres de alguna irregularidad dentro de tu proceso de denuncia, puedes reportarlas.
5. En caso de que acudas a la oficina incorrecta, el personal que te atienda debe orientarte sobre dónde denunciar. Recuerda que la Policía Cibernética Municipal puede orientarte y acompañarte a poner tu respectiva denuncia.

4 Datos sobre el hecho que son importantes y se deben mencionar

Lo principal que se debe explicar sobre el delito al funcionario que atienda su caso es lo siguiente:

- **¿Qué fue lo que ocurrió?**
- **¿Cómo fue que ocurrió?**
- **¿Cuándo ocurrió?**
- **¿Dónde ocurrió?**
- **¿Quién cometió el delito o sus características?**
- **¿En qué fecha y hora ocurrió?**

Enseguida el funcionario va a proceder a levantar un acta o carpeta de investigación con toda la información entregada.

5 Seguimiento a tu denuncia

Conoce como puedes dar seguimiento a tu denuncia y verificar que esta se realice debidamente:

- Antes de salir del lugar dónde realizaste tu denuncia de manera presencial, s**olicita copia de tu carpeta de investigación y anota el folio/número de tu carpeta de investigación también llamado CDI.**
- Recuerda que **tienes derecho a estar informado o informada sobre los avances y las decisiones que se tomen sobre tu caso y a oponerte a alguna decisión,** si no te convence o te perjudica.

6 Haz valer tus derechos

Si eres víctima de corrupción, o algún tipo de irregularidad, maltrato o te negaron información puedes reportar directamente con las autoridades que se encargan de vigilar, recibir quejas y sancionar el actuar de las y los funcionarios que trabajan en estas instituciones.

Puedes acudir a realizar tu reporte a la siguiente institución:

Comisión Nacional de Derechos Humanos.
Mariano Otero 685, San Luis Potosí, (+52 444 198 5000)

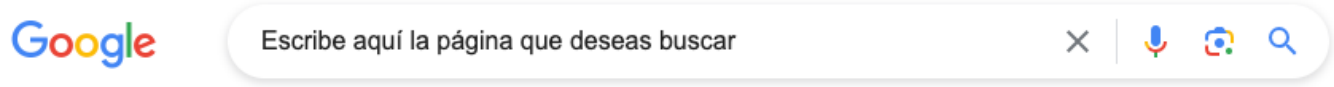
Aprende a guardar las pruebas

Es importante recabar toda la información que sea posible sobre el hecho, en este caso al ser un delito informático, puede que sean de utilidad conversaciones, imágenes, videos, páginas web o URL que podrán ser presentados al momento de realizar la denuncia.

Como docente puedes enseñar a tus estudiantes a guardar las pruebas si son víctimas de algún delito de tipo informático, enseñar a que autoridad pueden acudir y como se debe realizar el proceso de denuncia.

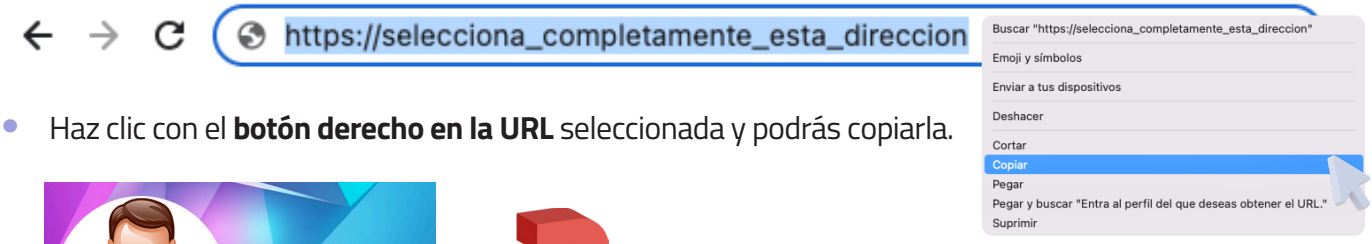
1 Para obtener un URL desde tu computadora

- En tu computadora, ve a tu buscador de preferencia y busca la página de la que deseas obtener el URL.



- En los resultados de la búsqueda, haz clic en el título de la página.

- En la parte superior del navegador, haz clic en la barra de direcciones para seleccionar la URL completa.



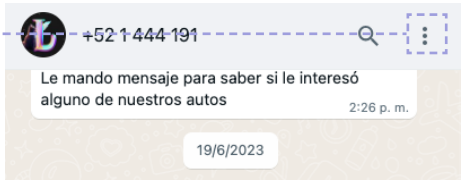
- Haz clic con el **botón derecho en la URL** seleccionada y podrás copiarla.

2 Para obtener un URL de un perfil de Facebook o Instagram en tu teléfono

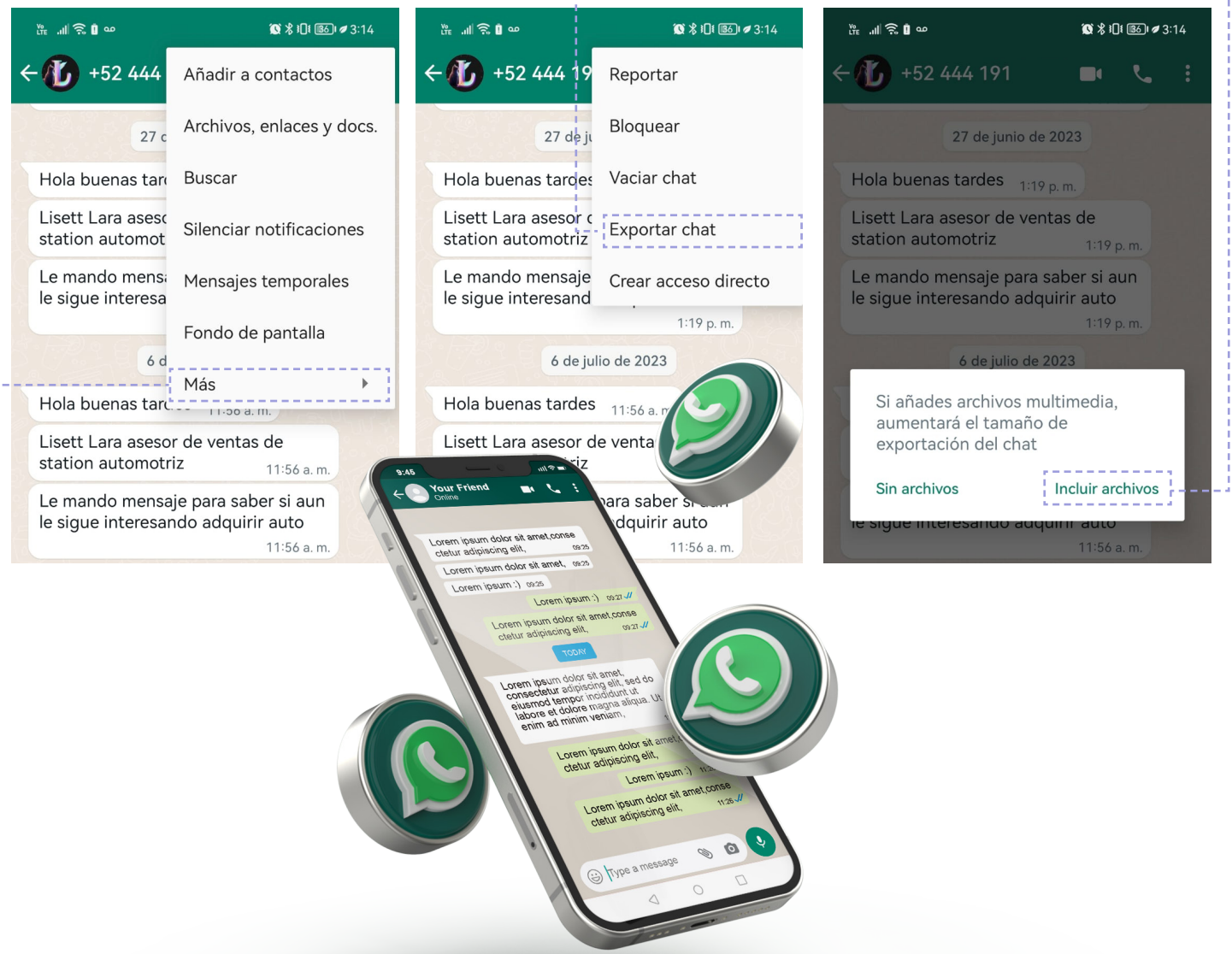
- Entra al perfil del que deseas obtener el URL.
- En el perfil, pulsa los tres puntos que se ubican junto al botón de "Te gusta" (si es una página) o "Enviar mensaje" (si es un perfil).
- Pulsa la opción de copiar enlace.

3 Exportar las conversaciones de un chat en WhatsApp

- Entra a la conversación de whataspp, debes dirigirte al ícono de tres puntos ubicado en la esquina superior derecha, pulsarlo y seleccionar ajustes.



- En la sección de ajustes debes seleccionar el apartado **Más** y pulsarlo.
- Selecciona la opción de **Exportar chat.**
- Selecciona **Incluir archivos** en caso de aparecer esa opción
- Guarda el archivo exportado.
- Recuerda que también puedes tomar captura de pantalla de la conversación.



3 TECNOLOGÍA, TU GRAN ALIADA

Tecnología, tu gran aliada

Algunas aplicaciones y consejos que te ayudarán.

Has llegado al apartado III de esta Guía, dentro de esta sección podrás encontrar múltiples herramientas que pueden facilitar el uso seguro de las TIC en tu institución y salón de clases, te proporcionaremos además algunos consejos sobre ciberseguridad y el uso responsable de las TIC.

Sin embargo, debes recordar que estas aplicaciones son un complemento en el labor docente y educativo para el desarrollo de habilidades del siglo XXI, además, cabe señalar que siempre deben ir acompañadas de actividades digitales en conjunto que puedan facilitar un clima de comunicación y confianza que promueva un uso seguro y responsable.

Estas a un paso de convertirte en un Defensor Digital, disfruta este último apartado y sé todo un experto en ciberseguridad.

¿Por qué es importante la ciberseguridad en mi escuela ?

Te presentamos una serie de afirmaciones que te ayudaran a recordar la importancia de la seguridad digital dentro del ámbito escolar y por supuesto en la vida diaria; **lee cuidadosamente cada sentencia y decide si la información es verdadera (V) o falsa (F).**

		V	F
1.	La seguridad digital en las escuelas es importante para fomentar la confianza y el respeto en línea lo que permite promover un entorno de aprendizaje seguro y saludable.		
2.	Los estudiantes deben ser instruidos en como proteger sus dispositivos y cuentas personales en línea para garantizar su proteger.		
3.	Las escuelas no tienen la responsabilidad de proteger la privacidad y la seguridad de los estudiantes en línea, ya que esto es responsabilidad de los padres.		
4.	Las escuelas deben proporcionar capacitación en seguridad digital no solo a los estudiantes, sino también al personal educativo y administrativo.		
5.	Las escuelas pueden utilizar herramientas de filtrado de contenido para bloquear el acceso a sitios web inapropiados o peligrosos en línea.		
6.	La colaboración entre estudiantes, padres y educadores es esencial para garantizar la seguridad en las TIC en las escuelas.		
7.	La educación en seguridad digital en las escuelas ayuda a los estudiantes a desarrollar habilidades y conocimientos que pueden aplicar en su vida personal y profesional.		
8.	La seguridad en las TIC es importante en las escuelas porque los estudiantes y el personal utilizan información personal y confidencial.		
9.	Las escuelas tienen la responsabilidad de proteger tanto a sus estudiantes como a su personal laboral sobre la exposición a contenido inapropiado o peligroso en línea.		
10.	La implementación de la seguridad digital puede ayudar a reducir el riesgo de ser víctima de algún incidente informático.		

Conoce las respuestas

1. La seguridad digital en las escuelas es importante para fomentar la confianza y el respeto en línea lo que permite promover un entorno de aprendizaje seguro y saludable.

VERDADERO

2. Los estudiantes deben ser instruidos en como proteger sus dispositivos y cuentas personales en línea para garantizar su proteger

VERDADERO

3. Las escuelas no tienen la responsabilidad de proteger la privacidad y la seguridad de los estudiantes en línea, ya que esto es responsabilidad de los padres.

FALSO

4. Las escuelas deben proporcionar capacitación en seguridad digital no solo a los estudiantes, sino también al personal educativo y administrativo.

VERDADERO

5. Las escuelas pueden utilizar herramientas de filtrado de contenido para bloquear el acceso a sitios web inapropiados o peligrosos en línea.

VERDADERO

6. La colaboración entre estudiantes, padres y educadores es esencial para garantizar la seguridad en las TIC en las escuelas.

VERDADERO

7. La educación en seguridad digital en las escuelas ayuda a los estudiantes a desarrollar habilidades y conocimientos que pueden aplicar en su vida personal y profesional.

VERDADERO

8. La seguridad en las TIC es importante en las escuelas porque los estudiantes y el personal utilizan información personal y confidencial.

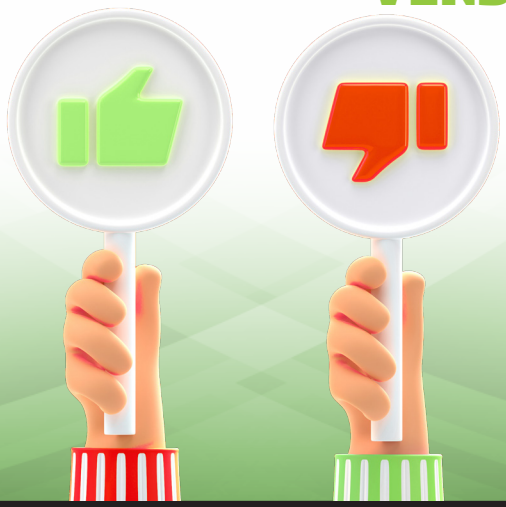
VERDADERO

9. Las escuelas tienen la responsabilidad de proteger tanto a sus estudiantes como a su personal laboral sobre la exposición a contenido inapropiado o peligroso en línea.

VERDADERO

10. La implementación de la seguridad digital puede ayudar a reducir el riesgo de ser víctima de algún incidente informático.

VERDADERO



Una herramienta que te será de mucha utilidad.

SafeSearch o Búsqueda Segura de Google

¿Para qué sirve?

Búsqueda Segura o SafeSearch puede ayudar a **filtrar el contenido explícito de los resultados de busqueda,** tanto si utilizas la Búsqueda de Google en el trabajo, con niños o en tu vida personal. Los resultados explícitos que seran filtrados incluyen contenido sexualmente explícito, como pornografía, violencia y violencia sangrienta.

Importante:

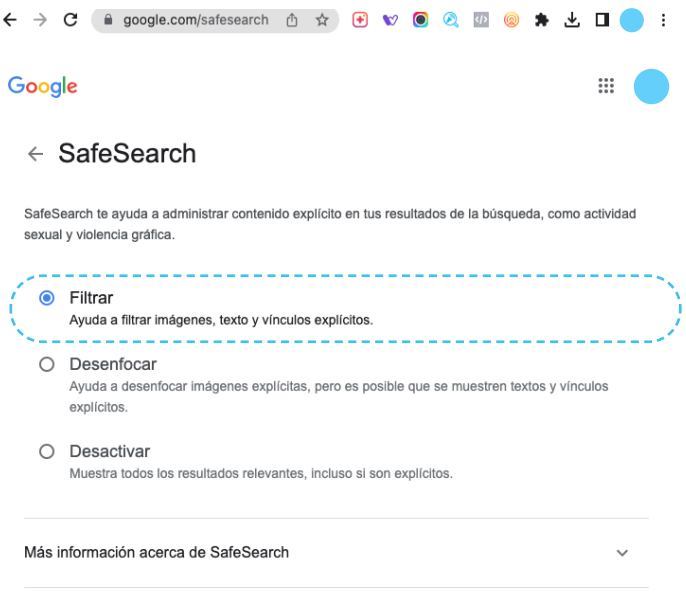
Búsqueda Segura solo funciona en los resultados de búsqueda de Google. No bloqueará el contenido explícito que encuentres en otros buscadores ni en sitios web que visites directamente.

Cómo activar o desactivar la Búsqueda Segura

Si gestionas tu cuenta de Google, puedes activar Búsqueda Segura en tu cuenta personal o en tu navegador.

- En tu computadora, ve a la configuración de Búsqueda Segura. **https://www.google.com/safesearch**
- Enseguida y de manera fácil y rápida podrás activar o desactivar la Búsqueda Segura.

Nota: En la parte superior derecha de los resultados de búsqueda de Google, también puedes hacer clic en Ajustes rápidos para activar o desactivar Búsqueda Segura.



Búsqueda Segura en una red que gestiones de un centro educativo

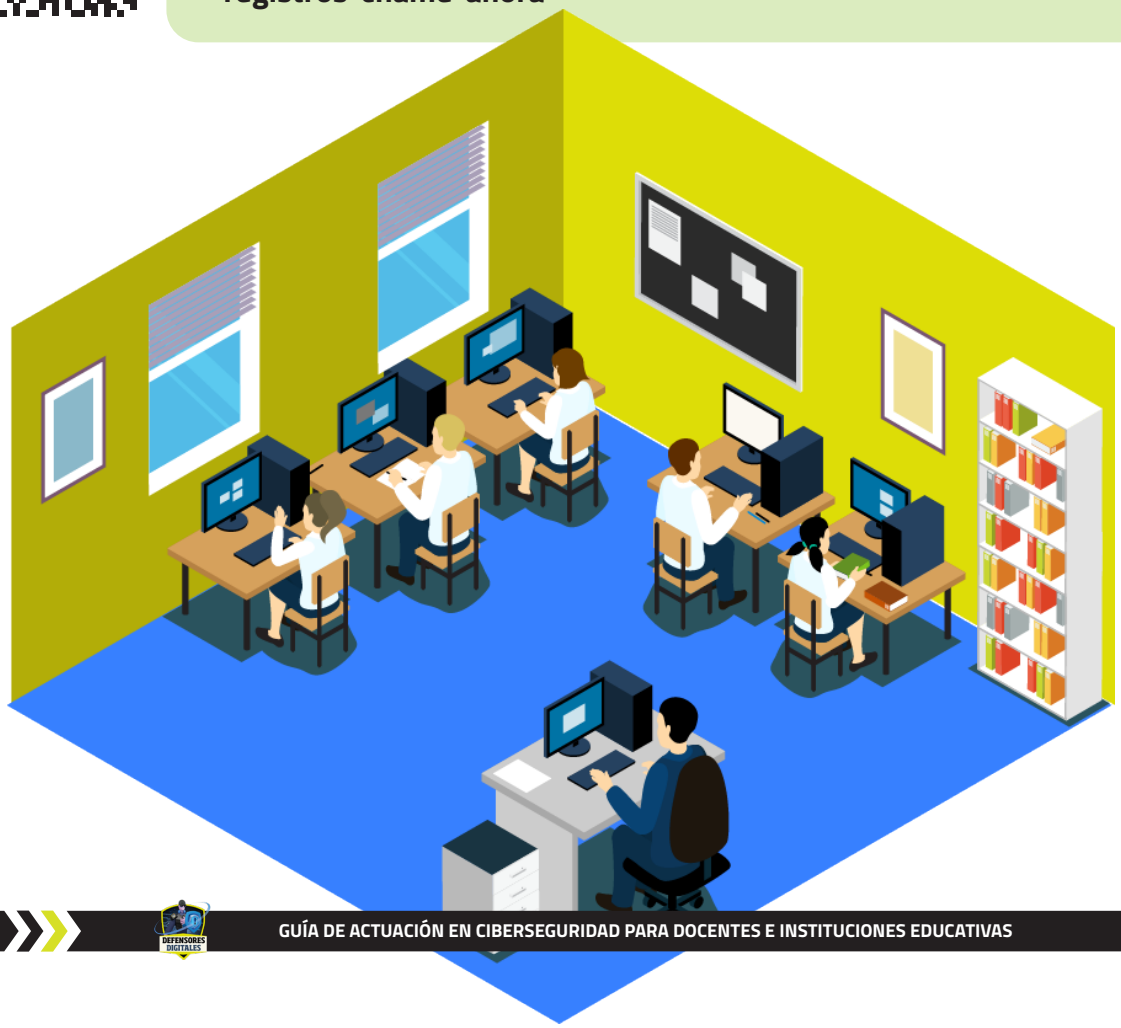
Si gestionas un centro educativo o alguna institución, puedes forzar que el ajuste "Búsqueda Segura" se encuentre activado en todos los navegadores y dispositivos que utilizan la red.

Se asignara una dirección IP virtual de Búsqueda Segura a todos los dominios de Google que incluyas en la configuración y no se podrá deshacer la configuración a nivel de navegador.

IMPORTANTE:

Para aplicar Búsqueda Segura en tu red, debes actualizar la configuración de DNS (Sistema de nombres de dominio). Configura la entrada de DNS de www.google.com como un CNAME (es un tipo de registro DNS que asigna un alias a un nombre de dominio auténtico o canónico) de forcesafesearch.google.com.

Google cuenta con un centro de ayuda ante cualquier problemática o duda, si quieres aventurarte por tu cuenta y conocer un poco más del tema, te compartimos el siguiente enlace de información. **https://support.google.com/a/answer/112037?hl=es-419#zippy=%2Cconfigurar-los-registros-cname-ahora**



Google Workspace for Education

Google Workspace for Education es un paquete de herramientas y servicios de Google ideado para centros educativos tradicionales y otras instituciones que imparten clases en casa para colaborar, agilizar la enseñanza y aprender de forma segura. Google Workspace for Education ofrece varias opciones para cumplir con las necesidades por ejemplo:

Controlar el acceso a los servicios de Google por edad

Para adaptar las experiencias a tus usuarios fácilmente, puedes configurar el acceso a algunos servicios de Google en función de su edad, el ajuste predeterminado de acceso por edad dependerá del tipo de institución educativa:

Instituciones de educación primaria y secundaria: todos los usuarios no designados como mayores de 18 años tendrán una experiencia restringida por edad en algunos servicios de Google.

Instituciones de educación superior: los usuarios no designados como menores de 18 años no tendrán restricciones adicionales en los servicios de Google. Sin embargo, los administradores de estas organizaciones deben identificar a todos los usuarios que tengan menos de 18 años.

Para configurar el acceso por edad:

1. **Primero debes iniciar sesión** en la consola de administración de Google, debes utilizar una cuenta de administrador, no tu cuenta personal.
2. En la página principal de la consola de administración, **haz clic en Configuración de la cuenta** después selecciona ajustes de acceso determinado por la edad.
3. Si deseas que el ajuste que elijas a continuación se aplique a todos los usuarios, debes mantener, deja seleccionado el nivel organizativo superior. De lo contrario, selecciona una unidad organizativa secundaria o un grupo de configuración.
4. **En Elige una etiqueta de edad adecuada, selecciona una opción:**
   - Algunos usuarios o todos tienen menos de 18 años
   - Todos los usuarios tienen 18 años o más
5. **Haz clic en Guardar.** Si has configurado una unidad organizativa o un grupo, puedes heredar o anular una unidad organizativa superior, o bien no definir ninguna opción en el caso de los grupos.ninguna opción en el caso de los grupos.

Google Workspace for Education es un paquete de herramientas y servicios de Google ideado para centros educativos y está disponible en todo el mundo para las instituciones educativas que cumplan los requisitos, si te llama la atención puedes revisar el siguiente enlace para ver todas sus funciones. **https://support.google.com/a/answer/2856827#signup**

¿Tus estudiantes usan redes sociales ?

CONOCE SUS POLÍTICAS DE USO

Las políticas de uso de las redes sociales son reglas establecidas por la plataforma que los usuarios deben seguir para garantizar una interacción segura y adecuada en línea, estas políticas establecen los límites para el contenido que se puede publicar, las conductas permitidas y prohibidas, así como las consecuencias de violar las normas.

Es importante conocer las políticas de uso de las redes sociales para evitar publicar contenido inapropiado o realizar conductas que puedan llevar a consecuencias negativas, como la suspensión o eliminación de la cuenta, además, estas políticas también pueden ayudar a los usuarios a protegerse de los riesgos en línea, como el acoso y el ciberacoso.

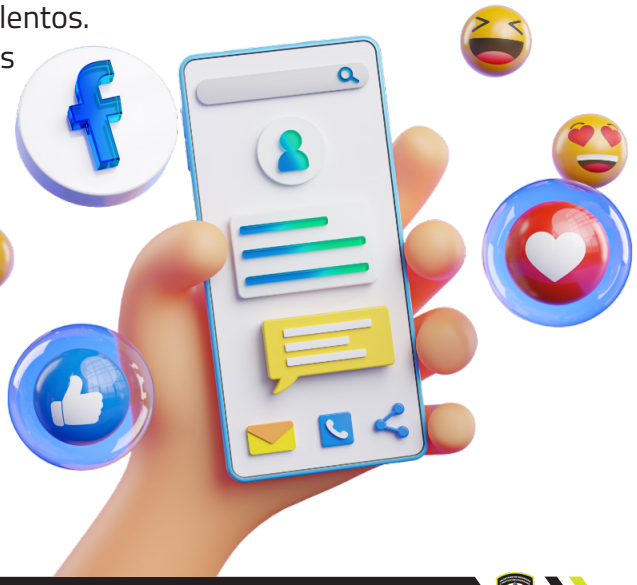
FACEBOOK

¿QUÉ PUEDES Y QUE NO PUEDES HACER?

La edad mínima establecida por la plataforma para ser usuario es de **13 años.**

No puedes usar la plataforma para realizar acciones o compartir contenidos:

- Que sean ilegales, engañosos, discriminatorios o fraudulentos.
- Que no sean de tu propiedad o no dispongas de los derechos.
- Que vulneren o infrinjan los derechos de otra persona.
- No puedes subir virus o código malicioso.
- No puedes sustituir, solicitar ni recopilar los nombres de usuario o contraseñas, ni apropiarte indebidamente de tokens de acceso.
- No puedes usar indebidamente los canales de reportes, marcado, disputas o apelaciones.
- Se recomienda que reportes contenido o cualquier comportamiento que consideres que infringe tus derechos.



INSTAGRAM

La edad mínima establecida por la plataforma para ser usuario es de **13 años.**

¿Qué puedes y qué no puedes hacer?

No puedes usar la plataforma para realizar acciones o compartir contenidos:

- No publiques información privada de otra persona.
- No uses Instagram para hacer nada ilegal.
- No acoses a nadie ni publiques nada feo sobre ninguna persona
- No uses la cuenta de nadie sin permiso, ni intentes descubrir sus datos de login.
- No publiques nada que muestre violencia, que pueda asustar a otras personas o que contenga imágenes con desnudos.
- No hagas nada que pueda afectar al modo en que otras personas usan y disfrutan de Instagram.

X (ANTES TWITTER)

¿Qué puedes y qué no puedes hacer?

La edad mínima establecida por la plataforma para ser usuario es de **13 años.**

No puedes usar la plataforma para realizar acciones o compartir contenidos:

- No puedes hacer amenazas violentas contra una persona o un grupo de personas.
- No puedes amenazar o fomentar el terrorismo o el extremismo violento.
- No puedes participar en situaciones de acoso dirigidas a una persona o incitar a otros a hacerlo.
- No puedes fomentar ni promover el suicidio o las autolesiones.
- No puedes publicar contenido multimedia que sea excesivamente morboso ni compartir contenido violento o para adultos en videos en vivo o en imágenes de perfil o encabezados.

Vincula Para Prevenir

Ejemplos de cómo usar las redes sociales para la educación

FACEBOOK

- Crea grupos privados para organizar debates.
- Crea grupos para juegos de rol en donde podrán asumir diferentes roles para empatizar y respetar a otros.
- Puedes compartir los trabajos y proyectos hechos en clase.

X (ANTES TWITTER)

- Búsqueda de Fake news.
- Generar contenido para estudio por medio de tuiteo.

INSTAGRAM

- Documentar un tema por medio de fotografías.
- Realizar redacciones a partir de fotos compartidas por personajes importantes.
- Localizar imágenes para situar en mapas geográficos.

YOUTUBE

- Presentación de trabajos (con grabación y edición de videos)
- Búsqueda de información por medio de documentales.
- Escucha de otros idiomas por medio de canciones, entrevistas, clips, narraciones, audiolibros, etc.

TIK TOK

- Clases en directo.
- Creación de videos con contenido educativo.
- Replica de experimentos (con supervisión).

Grupos de WhatsApp

Una herramienta para el docente digital

Ventajas

Comunicación en tiempo real: Las madres, padres y cuidadores pueden comunicarse directamente con los maestros y obtener respuestas rápidas a sus preguntas o inquietudes, además, los docentes pueden enviar actualizaciones importantes en tiempo real, como cambios de horario o recordatorios de tareas.

Colaboración y apoyo: Las madres, padres y cuidadores pueden compartir recursos o información útil con los maestros, y los maestros pueden pedir ayuda o sugerencias a estos, lo que puede ayudar a crear una comunidad colaborativa y solidaria.

Seguimiento del progreso del estudiante: Los maestros pueden compartir actualizaciones sobre el progreso del estudiante, lo que permite a madres, padres y cuidadores mantenerse informados y hacer un seguimiento del rendimiento académico de sus hijos.

Solución de problemas: Si surge algún problema, los padres pueden comunicarse directamente con los maestros y trabajar juntos para resolverlo de manera rápida y efectiva.

Inconvenientes

Dificultad para mantener la privacidad: Es importante asegurarse de que la información compartida en el grupo sea confidencial y se comparta solo con las personas adecuadas, sin embargo, esto puede ser difícil de garantizar en un grupo de WhatsApp, especialmente si hay muchos miembros.

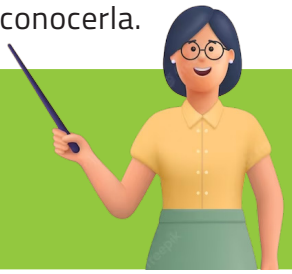
Dificultad para mantener el respeto: En un grupo de WhatsApp, puede haber mensajes inapropiados, comentarios fuera de lugar o discusiones acaloradas, es importante establecer reglas claras para asegurarse de que todos los miembros se comuniquen de manera respetuosa y profesional.

Distracciones en el aula: Si los maestros están revisando constantemente el grupo de WhatsApp en el aula, puede haber distracciones en la enseñanza y el aprendizaje. Además, si los padres envían mensajes durante las horas de clase, puede haber interrupciones en la atención de los estudiantes.

Posible falta de inclusión: Es importante tener en cuenta que no todos tienen acceso o están familiarizados con la tecnología y las aplicaciones de mensajería como WhatsApp, por lo tanto, si se utiliza un grupo de WhatsApp como la única forma de comunicación, puede haber madres, padres y cuidadores que se sientan excluidos o que no reciban información importante, asegúrese de que todos tengan acceso a la información de manera equitativa y justa.

¿Qué puedes hacer como docente al encontrar problemáticas dentro de estos grupos?

Es importante tener en cuenta que el grupo de WhatsApp debe ser utilizado de manera responsable y respetuosa, es necesario establecer reglas claras para la comunicación y asegurarse de que todos los miembros se adhieran a ellas, además, la privacidad de los estudiantes debe ser protegida y se debe asegurar que cualquier información personal se comparta solo con los miembros del grupo que necesiten conocerla.



Si detectas alguna problemática dentro del grupo de WhatsApp es importante que tomes medidas para resolver el problema.

Aquí te presento algunos pasos que puedes seguir

1. **Identifica el problema:** Antes de tomar cualquier acción, debes identificar el problema específico que está ocurriendo en el grupo. Esto te ayudará a entender cuál es la causa raíz del problema y cómo abordarlo.

2. **Habla con los involucrados:** Si detectas que hay algún mensaje inapropiado o contenido que no debería estar en el grupo, habla con los involucrados en privado. Se claro y respetuoso al explicar la situación y pide que se elimine el contenido inapropiado.

3. **Modera el grupo:** Si el problema persiste, puede ser necesario que tomes medidas más drásticas, como moderar el grupo de manera activa. Esto significa que puedes eliminar mensajes inapropiados o incluso expulsar a un miembro del grupo si es necesario.

4. **Enfócate en las soluciones:** En lugar de centrarse en el problema en sí, enfócate en las posibles soluciones. Trata de encontrar una solución que satisfaga a todas las partes involucradas y que respete las reglas establecidas en el grupo.

5. **Sé imparcial:** Como maestro, es importante mantener una posición imparcial en cualquier problema que surja en el grupo. Escucha a todas las partes involucradas y trata de entender sus perspectivas antes de tomar una decisión.

6. **Si es necesario, elimina a un miembro del grupo:** Si un miembro del grupo no respeta las reglas establecidas o causa problemas constantemente, es posible que tengas que eliminarlo del grupo, sin embargo, asegúrate de explicar la razón detrás de esta decisión.

Las reglas del grupo

Al comienzo de la creación del grupo, es importante establecer reglas claras y definir el propósito del grupo, las reglas deben incluir el uso apropiado del lenguaje, el respeto hacia los demás miembros, la no divulgación de información confidencial y la prohibición de compartir contenido inapropiado.

Establecer estas reglas y difundirlas de manera clara entre las madres, padres y cuidadores incluso de manera digital, ayudará a facilitar tu actuación en caso de alguna problemática, funcionando como un antecedente de un uso apropiado.

Reglas para el buen uso del grupo de WhatsApp de madres, padres y cuidadores

Recuerda que la finalidad del grupo es mejorar la comunicación para beneficio de los estudiantes.

- Utiliza el grupo solo para asuntos relacionados con la educación y la escuela.
- Nunca utilices el grupo para criticar, insultar o difamar a los docentes, a otras madres, padres o cuidadores y mucho menos a los estudiantes.
- Dirige cualquier queja o sugerencia directamente al profesorado, no trates de solucionarlo en el grupo.
- Utiliza el grupo solo para cuestiones que afecten a todas las alumnas y alumnos.
- Escribe solo información relevante y evita la difusión de imágenes o vídeos de los docentes, otras madres, padres o cuidadores y mucho menos a los estudiantes.
- No compartas contenido multimedia sin verificar su origen y su veracidad.
- Mantén la privacidad de la información compartida en el grupo, evitando compartir información personal o confidencial.
- No compartas contenido multimedia sin verificar su origen y su veracidad.

Resolución
De conflictos

La mediación escolar es una herramienta importante para resolver problemas en la escuela, como docente, debes asegurarte de que los estudiantes involucrados en algún problema se sientan escuchados y que se llegue a un acuerdo justo y efectivo, además, es importante trabajar en la prevención promoviendo un ambiente escolar seguro, respetuoso y sin violencia en línea o de manera física.

1. **Identificación del problema:** como maestro, debes identificar la situación que se está presentando entre tus estudiantes, esto implica hablar con los estudiantes involucrados, recopilar información sobre lo que sucedió y cómo se sienten las personas afectadas.

2. **Convocatoria a la mediación:** una vez que hayas identificado el problema, debes convocar a una mediación en la que estén presentes los estudiantes involucrados, sus padres y otros miembros del equipo escolar que puedan apoyar en el proceso, de igual manera puedes apoyarte por personal especializado de Policía Cibernética Municipal.

3. **Establecimiento de las reglas:** en la mediación, debes establecer las reglas básicas de la comunicación, como por ejemplo, que los estudiantes se turnen para hablar y que se escuchen mutuamente sin interrumpir.

4. **Escucha activa:** debes permitir que cada estudiante exprese sus sentimientos y su versión de los hechos. Es importante escuchar con atención, demostrar empatía y validar los sentimientos de cada persona.

5. **Identificación de soluciones:** en la mediación, deben identificarse posibles soluciones al problema, como disculpas, cambios en el comportamiento, reparación del daño causado, etc.

6. **Acuerdo:** una vez que se han identificado las soluciones, es importante que los estudiantes involucrados lleguen a un acuerdo sobre las acciones que tomarán para resolver el problema.

7. **Seguimiento:** finalmente, es importante hacer un seguimiento del acuerdo y del proceso de mediación para asegurarse de que se esté cumpliendo y que el problema se haya resuelto de manera efectiva.

Instituciones amigas

¿Dónde puedes pedir ayuda?

Es importante que conozcas las autoridades a las que pueden acudir en caso de detectar un incidente/delito informático o alguna otra problemática de esta índole en su escuela, ya que esto les permitirá tomar medidas adecuadas para protege a niñas, niños y adolescentes.

Policía Cibernética de la Secretaría de Seguridad y Protección Ciudadana del Municipio de San Luis Potosí

La Policía Cibernética de la Secretaría de Seguridad y Protección Ciudadana del Municipio de San Luis Potosí es una jefatura que cuenta con personal capacitado en incidentes de tipo informático.

¿En dónde puedo contactarlos?

¿Buscas asesoría de manera personal?, visítanos:
Calle 6ª. Oriente No. 455, Col. Central de Abastos, San Luis Potosí, S.L.P

¿Deseas una atención telefónica o por WhatsApp? Comunícate:
444-329-32-81

¿Prefieres usar facebook?, mándanos mensaje:
Policía Cibernética Municipal SSPC SLP.
https://www.facebook.com/Ciber.SSPC

¿Instagram es tu app favorita?, también estamos ahí:
Ciber.sspcslp.
https://instagram.com/ciber.sspcslp?igshid=Yzg5MTU1MDY=

¿Quizás prefieres una atención por Twitter?, adelante:
@Ciber_SSPCSLP
https://twitter.com/Ciber_SSPCSLP

Estamos en todos lados, contáctanos en telegram:
444-329-32-81

También puedes contactarnos por correo:
policiacibernetica@sanluis.gob.mx

No estaría mal que nos contactaras también por Tik Tok:
ciber.sspcslp
https://www.tiktok.com/@ciber.sspcslp?is_from_webapp=1&sender_device=pc

PUERTA VIOLETA

¿En dónde puedo contactarlos?

Es una Unidad de Atención Multiagencial para Mujeres que responde a la necesidad de las mujeres de contar con espacios de atención y protección integrales, especializadas y con perspectiva de género, porque los delitos cibernéticos muchas veces requieren atención focalizada.

¿BUSCAS ASESORÍA DE MANERA PERSONAL?, ADELANTE:
Uresti 555, Centro Historico, 78000 San Luis, S.L.P.

LÍNEA DE ATENCIÓN DE "PUERTA VIOLETA"
444-139-07-20

Glosario de términos

Quieres conocer algunos términos de la vida digital y la ciberseguridad, aquí tenemos algunos para ti. ¡Échales un vistazo!

Antivirus
Software de protección para evitar que ejecutemos algún tipo de malware en nuestro equipo que infecte al equipo.

AUTENTICACIÓN
Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico, etc.

CIBERESPACIO
Cuando hablamos del ciberespacio hacemos referencia al espacio virtual en donde las personas por medio de un software consumen los servicios de Internet como las redes sociales, correos, sitios web y todo lo que puedas encontrar en línea.

CIBERSEGURIDAD
Es un término sumamente importante pues habla de la protección de tus datos, tu confidencialidad y tu integridad dentro del ciberespacio.

INGENIERÍA SOCIAL
Es aquella práctica utilizada para obtener tu información o intentar que realices alguna acción usando técnicas de manipulación que pueden parecer aparentemente inofensivas, pero lo que buscan la mayoría de las veces es perjudicarte.

INTERNET
Es la red mundial que permite acceder a toneladas de información desde cualquier parte del mundo, nos permite comunicarnos con otras personas sin la necesidad de estar frente a frente y de manera casi instantánea, así como muchas cosas más.

MALWARE
Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

SOFTWARE
Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo, conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas.

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)
Las TIC´s son todas aquellas tecnologías requeridas para almacenar información, comunicarnos, recuperar datos e informarnos, siendo algunos ejemplos el teléfono, los celulares, la imprenta, el correo, las computadoras y el más popular, internet.

¿Quiéres conocer un poco más?

Consulta el glosario en el siguiente enlace, o escanea el código QR:
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Referencias

- (2010). Nativos Digitales: Desafio de la educación actual. Paradígma, 31(2), 5-6. Recuperado en 15 de diciembre de 2022, de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1011-22512010000200001&lng=es&tlng=es.
- Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacionaly su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia, 25(89), 351-368.
- Armero Pedreira, P., Bernardino Cuesta, B., & Bonet de Luna, C. (2011). Acoso escolar. Pediatría Atención Primaria, 13(52), 661-670. https://dx.doi.org/10.4321/S1139-76322011000600016
- Belloch C. Las tecnologías de la información y comunicación en el aprendizaje. Material docente [en línea]. Universidad de Valencia, Departamento de Métodos de Investigación y Diagnóstico en Educación; 2012. http://www.uv.es/bellochc/pedagogia/EVA1.pdf
- Calle González, Silvia, Torres Belduma, Karen, & Tusa Jumbo, Fernanda. (2022). Las TICs, la enseñanza y la alfabetización digital de la familia. Transformación, 18(1), 94-113. Epub 01 de enero de 2022. Recuperado en 14 de diciembre de 2022, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2077-29552022000100094&lng=es&tlng=es.
- Convención Sobre Los Derechos Del Niño, 20 de noviembre de 1989. https://www.un.org/es/events/childrenday/pdf/derechos.pdf
- Equipo de Expertos en Educación. (7 diciembre 2014). Los perfiles tipo en el bullying: víctima, agresor, instigadores y espectadores pasivos. Valencia. Universidad Internacional de Valencia. https://www.universidadviu.com/es/actualidad/nuestros-expertos/los-perfiles-tipo-en-el-bullying-victima-agresor-instigadores-y
- Fajardo Caldera, M. I., Gordillo Hernández, M., & Regalado Cuenca, A. B. (2013). SEXTING: NUEVOS USOS DE LA TECNOLOGÍA Y LA SEXUALIDAD EN ADOLESCENTES. International Journal of Developmental and Educational Psychology, 1(1), 521-533.
- Flores Quispe, C. TIPOS DE HACKERS. RITS, La Paz,n. 8, June 2013. http://www.revistasbolivianas.ciencia.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100008&lng=en&nrm=iso>. access on 21 Dec.2022.
- (Fundación Save the Children. (09 Julio 2019). HAPPY SLAPPING CUANDO LA VIOLENCIA SE HACE VIRAL. https://www.savethechildren.es/actualidad/happy-slapping-violencia-online-menores
- García-Córdoba, J, & Herrero-Pérez, L. (2020). La ciberdefensa en los sistemas de información sanitarios militares. Sanidad Militar, 76(3), 140-142. Epub 08 de marzo de 2021.https://dx.doi.org/10.4321/s1887-85712020000300001
- Gil Juliá, Beatriz; Castro Calvo, Jesús; Ruiz Palomino, Estefanía; García Barba, Marta; Ballester Arnal, Rafael. (2018). CONSECUENCIAS DE LA EXPOSICIÓN INVOLUNTARIA A MATERIAL SEXUAL EN ADOLESCENTES. International Journal of Developmental and Educational Psychology, vol. 2, 1. https://www.redalyc.org/articulo.oa?id=349856003003

- Gil-Juliá, B., Castro-Calvo, J., Ruiz-Palomino, E., García-Barba, M., & Ballester-Arnal, R. (2018). Consecuencias de la exposición involuntaria a material sexual en adolescentes. Revista INFAD De Psicología. International Journal of Developmental and Educational Psychology., 2(1), 33–44. https://doi.org/10.17060/ijodaep.2018.n1.v2.1159
- Heinze Martin, Gerhard, Olmedo Canchola, Víctor Hugo, & Andoney Mayén, Jéssica Valeria. (2017). Uso de las tecnologías de la información y comunicación (TIC) en las residencias médicas en México. Acta médica Grupo Ángeles, 15(2), 150-153. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-72032017000200150&lng=es&tlng=es.
- Ibarra López, A. M., & Llata Gómez, D. E. (2010). NIÑOS NATIVOS DIGITALES EN LA SOCIEDAD DEL CONOCIMIENTO: ACERCAMIENTOS CONCEPTUALES A SUS COMPETENCIAS. Razón y Palabra, (72).
- https://www.unodc.org/documents/ropan/2020/Ciberdelito_junio2020/SEXTORSION.pdf
- Internet Segura for Kids (IS4K). (S/F). HERRAMIENTAS DE CONTROL PARENTAL. https://www.is4k.es/de-utilidad/herramientas
- Jones, L., Mitchell, K. y Finkelhor, D. (2012). Trends in youth Inernet victimization: Findings from three youth Internet safety surveys 2000-2010. Journal of Adolescent Health, 50, 179-186. http://dx.doi.org/10.1016/j.jadohealth.2011.09.015
- Lugones Botell, Miguel, & Ramírez Bermúdez, Marieta. (2017). Bullying: aspectos históricos, culturales y sus consecuencias para la salud. Revista Cubana de Medicina General Integral, 33(1), 154-162. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-21252017000100014&lng=es&tlng=es.
- Luisa Santillán, M. (12 de enero del 2015). Ciberbullying: perfil de víctimas y victimarios. México. CienciaUNAM.
- https://ciencia.unam.mx/leer/418/Ciberbullying_perfil_de_victimas_y_victimarios
- Instituto Nacional de Estadística y Geografía. (2021). Módulo sobre Ciberacoso (MOCIBA) 2021. https://www.inegi.org.mx/programas/mociba/2021/
- Moreno López, N., et. al. (2017). Alfabetización digital a padres de familia en el uso de las redes sociales. ALTERIDAD REVISTA DE EDUCACIÓN. Vol. 12 Núm. 1. https://www.redalyc.org/journal/4677/467751868001/html/
- Olweus D. Acoso escolar, "bullying", en las escuelas: hechos e intervenciones. www.acosomoral.org/pdf/Olweus.pdf
- Pérez Herrero, M. D., & Martínez González, R. (2006). EDUCACIÓN FAMILIAR Y TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN. International Journal of Developmental and Educational Psychology, 2(1), 567-576.
- Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad URVIO, Revista Latinoamericana de Estudios de Seguridad, núm. 20, pp. 80-93. https://www.redalyc.org/journal/5526/552656641007/html/
- REA, Asociación Castellano-Leonesa para la defensa de la Infancia y la Juventud. (2022). Buenos tratos en la pareja adolescente Vol. I – Ciberviolencia en la pareja. https://www.asociacionrea.org/buenos-tratos-en-la-pareja-adolescente-vol-i-ciberviolencia-en-la-pareja/

- Resett, Santiago. (2019). Sexting en adolescentes: su predicción a partir de los problemas emocionales y la personalidad oscura. Escritos de Psicología (Internet), 12(2), 93-102. Epub 09 de noviembre de 2020.https://dx.doi.org/10.24310/espsiescpsi.v12i2.10060
- Santisteban, Patricia de, & Gámez-Guadix, Manuel. (2017). Estrategias de persuasión en grooming online de menores: un análisis cualitativo con agresores en prisión. Psychosocial Intervention, 26(3), 139-146. https://dx.doi.org/10.1016/j.psi.2017.02.001
- Serrano Santoyo, A.; Martínez Martínez, E. (2003). La brecha digital: mitos y realidades. México: Editorial UABC. http://labrechadigital.org/labrecha/LaBrechaDigital_MitosyRealidades.pdf
- Smith KP. Ciberacoso: naturaleza y extensión de un nuevo tipo de acoso dentro y fuera de la escuela. Congreso Educación Palma de Mallorca, 2006.
- UNICEF Fondo de las Naciones Unidas para la Infancia, (2022), UNICEF PARA CADA INFANCIA, https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo
- https://www.inegi.org.mx/programas/dutih/2022/#informacion_general
- https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf
- https://www.inegi.org.mx/programas/mociba/2022/
- https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf
- https://www.inegi.org.mx/contenidos/programas/mociba/2022/doc/mociba2022_resultados.pdf
- https://www.inegi.org.mx/contenidos/programas/envipe/2023/doc/envipe2023_2_caracterizacion_delitos.pdf
- https://krimera.es/happy-slapping-conducta-ciberbullying/

Gabinete que construye la política pública

Mtro. Enrique Francisco Galindo Ceballos
Presidente Municipal

Comisario. Mtro. Juan Antonio de Jesús Villa Gutiérrez
Secretario de Seguridad y Protección Ciudadana

Subinspector. Mtro. Erick Javier de León Abundis
Director General de Tecnologías e Inteligencia Social

Mtro. Servando López Contreras
Director de Inteligencia Social

Lic. Pamela Andrea Cano Urbina
Jefa de Política Criminológica para la Atención de Delitos de Mayor Incidencia

Directorio

JEFATURA DE POLICÍA CIBERNÉTICA

Pol. 3° Guillermo Gamboa Rodríguez
Pol. 3° Miguel Gómez Hernández
Pol. Claudia Gómez Pinal
Pol. Alma Yadira Rodríguez De León
Pol. Olivia Esperanza Méndez Miranda
Pol. Emmanuel Medina García

JEFATURA DE POLÍTICA CRIMINOLÓGICA PARA LA ATENCIÓN DE DELITOS DE MAYOR INCIDENCIA

Lic. Consuelo Cabriales Guerrero

SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA

San Luis PotoSí

San Luis PotoSí

GOBIERNO DE LA CAPITAL

H. AYUNTAMIENTO DE SAN LUIS POTOSÍ 2024-2027

San Luis amable

sanluis.gob.mx

@slpmunicipio

unesco

Miembro de la Red Mundial de Ciudades del Aprendizaje