DEFENSORES DIGITALES

GUÍA DE ACTUACIÓN EN CIBERSEGURIDAD PARA MADRES, PADRES Y TUTORES

H. AYUNTAMIENTO DE SAN LUIS POTOSÍ 2024-2027

San Luis amable

sanluis.gob.mx

@slpmunicipio

Índice

    - **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**
- **Recordemos en dónde puedes reportar contenido**
- **Algunas páginas y Apps de riesgo, ¿Tu hija o hijo las usa?**
    - 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
    - Páginas de compra y ventafraudes en compra por internet
- **Ya conozco los riesgos... ¿Ahora que hago?**
- **¿Presentarás una denuncia?, te diremos cómo hacerlo**

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

- **Cierto o falso sobre los controles parentales**
    - Conoce las respuestas.
- **Control parental en 05 minutos o menos.**
    - Family Link
    - Family Time
    - Securekids
    - Life360
- **Control parental en redes sociales y Políticas de uso**
    - Facebook
    - Instagram
    - Tik Tok
    - Youtube
    - Uber, indriver o alguna otra app de transporte
- **Control parental en consolas de Videojuegos**
    - Videojuegos y sus categorías
    - Control familiar Microsoft
    - Control familiar XBOX
    - Control familiar Nintendo Switch
    - Control familiar Playstation
    - 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 madres, padres y cuidadores, 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 cultvural 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**

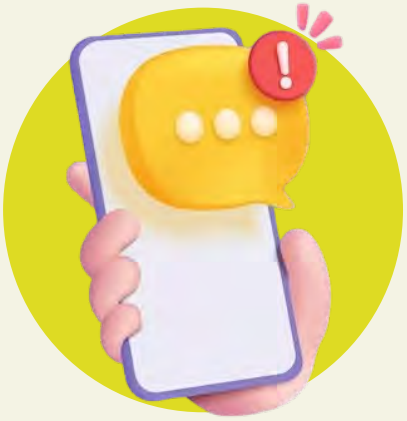
78.6%

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, mientas 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

¿Para que usan Internet?: Cifra en porcentaje



94.7 PARA COMUNICARSE.

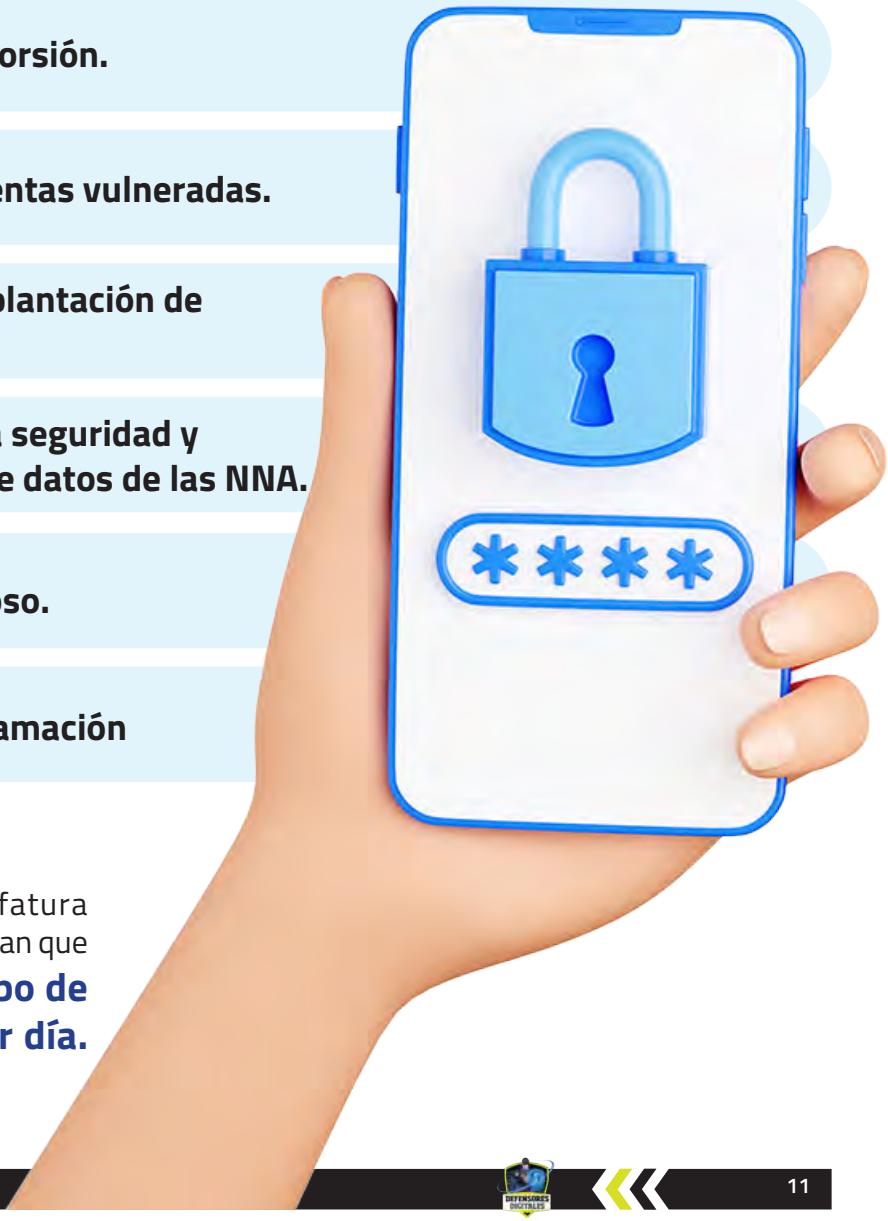
89.8 PARA ACCEDER A REDES SOCIALES.

89.6 PARA BUSCAR INFORMACIÓN.

85.7 PARA ENTRETENIMIENTO.

La Jefatura de Policía Cibernética del Municipio de San Luis Potosí ha detectado dentro de los primeros tres meses del año 2023, un total de **193 incidentes** relacionados con el uso de las Tecnologías de la información y comunicación (TIC):

33	**Casos de fraude.**
28	**Casos de extorsión.**
28	**Casos de cuentas vulneradas.**
26	**Casos de suplantación de identidad.**
14	**Garantizar la seguridad y protección de datos de las NNA.**
11	**Casos de acoso.**
8	**Casos de difamación**



193 incidentes registrados por la jefatura durante los primeros 72 días del año, señalan que de manera aproximada **se llevan a cabo de 2 a 3 incidentes cibernéticos por día.**

1 DEFENSORES DIGITALES

Compendio de actuación en ciberseguridad para madres, padres y cuidadores

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 comenzar un diálogo continuo 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.

Te invitamos a que te adentres a este Compendio y conozcas sobre ciberseguridad.

Lista de Verificación en Ciberseguridad

¿Estás seguro de que tienes prácticas seguras al usar la tecnología? **¡Vamos a averiguarlo!**

Conocer sobre tu vida digital te permitirá saber que debes trabajar para ser todo un Defensor digital.

Marca el recuadro que más se adecue a tus respuestas. ¡Adelante!

Mis dispositivos cuentan con un sistema de bloqueo para acceder (contraseñas, PIN, huella dactilar, patrón, etc.).		
Solo yo conozco el sistema de bloqueo y desbloqueo de mi dispositivo.		
Uso constantemente el antivirus para analizar mis dispositivos en busca de virus y malwares.		
He comprobado que todas mis contraseñas son seguras.		
Se encuentra instalado y activado un antivirus en mis dispositivos.		
Tengo activada la verificación en dos pasos en las aplicaciones que lo permiten, para tener aun más seguras y confiables mis cuentas.		
Mis dispositivos cuentan únicamente con aplicaciones y programas instalados de páginas oficiales como Play Store.		
Antes de instalar alguna aplicación compruebo los comentarios sobre ella y las valoraciones que han dado otros usuarios.		
Elimino todas las aplicaciones que ya no utilizo y además, son innecesarias en mis dispositivos.		

Antes de instalar una nueva aplicación reviso los permisos que solicita y estoy consciente de ellos.

Conecto mis dispositivos únicamente a redes WiFi seguras.

En caso de usar un dispositivo distinto al mío, siempre navego en modo privado.

Me conecto solo a páginas web seguras, confiables y me aseguro de comprobarlo cada que navego en Internet.

Cuento con un horario establecido para usar mis dispositivos.

Mis cuentas en redes sociales están configuradas para proteger mi seguridad y privacidad.

Mis publicaciones solo son visibles para mis contactos más cercanos.
Estoy consiente de lo que comparto, lo que veo en Internet y con

quién hablo.
Las publicaciones de mis redes sociales no contienen información

sensible o personal como direcciones, ubicación, datos bancarios, contraseñas, números de teléfono, etc.

Conozcamos tus resultados

Recuerda que mantenerte informado es la mejor defensa contra los riesgos de una vida digital.

¡Nunca es tarde para estar ciberseguro!

14-18 RESPUESTAS AFIRMATIVAS

Estoy listo para ser un Defensor Digital

¡Increíble!, Te encuentras ciberseguro, recuerda no bajar la guardia y seguir mejorando día con día tu seguridad y la de tu familia dentro de la vida online, no olvides mantenerte informado y alerta.

7-13 RESPUESTAS AFIRMATIVAS

Sólo un estirón más

Vas muy bien, pero siempre se puede mejorar, toma en cuenta tus respuestas y vamos manos a la obra con las acciones que te faltan, poco a poco puedes tener a toda tu familia cibersegura, recuerda que la información es tu mejor defensa.

1-6 RESPUESTAS AFIRMATIVAS

Quizás podamos darte algunos tips

Tranquilo, nunca es tarde para estar ciberseguro, mantenerte al tanto de las herramientas tecnológicas te permitirá aprovecharlas a tu favor y este compendio puede ayudarte con esa tarea, diviértete mientras te conviertes en un defensor digital.

Consejos y Datos Iniciales

¡Les damos la bienvenida a este Compendio!, sabemos que estás interesado en la ciberseguridad de tu familia, y para comenzar queremos darte algunos consejos que te permitirán conocer lo que involucra la vida digital y cómo convertirte en todo un defensor digital.

Sabemos que hoy en día es raro que no dispongamos de al menos un teléfono móvil con conexión a Internet para comunicarnos con nuestros familiares y amigos, quizás además tengamos una computadora o una tableta con la que nuestras hijas e hijos navegan por la red, juegan y aprenden.

La cantidad de información que almacenan estos dispositivos sobre las personas es enorme debido al uso diario que hacemos de ellos, por eso es tan importante que aprendamos a salvaguardar y proteger nuestros dispositivos de terceras personas con malas intenciones o para evitar que otras personas puedan acceder a su contenido sin nuestra autorización.

Queremos guiarte en este proceso de aprendizaje, así que conoce de todo lo que hay que saber y disfruta esta guía.

Lista de verificación en ciberseguridad

Para niñas, niños y adolescentes

Conocer sobre la vida digital de tus hijas e hijos te permitirá atender de manera especifica situaciones que pueden vulnerar su seguridad digital.

Te recomendamos contestar la siguiente lista junto a tus hijas e hijos, recuerda marcar el recuadro que más se adecue a las respuestas . ¡Adelante!

Los dispositivos de mi hija/hijo cuentan con un sistema de bloqueo para acceder (contraseñas, PIN, huella dactilar, patrón, etc.).		
Ademas de mi hija/hijo, solo yo conozco el sistema de bloqueo y desbloqueo de sus dispositivos.		
He comprobado que todas sus contraseñas son seguras.		
Se encuentra instalado y activado un antivirus en los dispositivos de mi hija/hijo.		
Los dispositivos de mi hija/hijo cuentan únicamente con aplicaciones y programas instalados de páginas oficiales como Play Store.		
Mi hija/hijo tiene activada la verificación en dos pasos en las aplicaciones que lo permiten, para tener aun más seguras y confiables sus cuentas.		
Antes de instalar alguna aplicación apoyo a mi hija/hijo a comprobar los comentarios y las valoraciones que han dado otros usuarios para ver si es segura.		
Antes de instalar una nueva aplicación apoyo a mi hija/hijo a revisar los permisos que solicita y ha estar consciente de ellos.		
Mi hija/hijo cuenta con un horario establecido para usar sus dispositivos.		

En caso de usar un dispositivo distinto al suyo, ti hija/hijo siempre navega en modo privado.		
Mi hija/hijo se conecta solo a páginas web seguras, confiables y se asegura de comprobarlo cada que navega en Internet.		
Sus cuentas en redes sociales están configuradas para proteger su seguridad y privacidad.		
Sus publicaciones solo son visibles para sus contactos más cercanos.		
Mi hija/hijo esta informado y es consiente de lo que comparte, lo que ve en Internet y con quién habla.		
Las publicaciones de sus redes sociales no contienen información sensible o personal, como direcciones, ubicación, contraseñas, números de teléfono, etc.		
Mi hija/hijo conoce los riesgos que existen en Internet y nos ayudamos mutuamente a estar ciberseguros.		

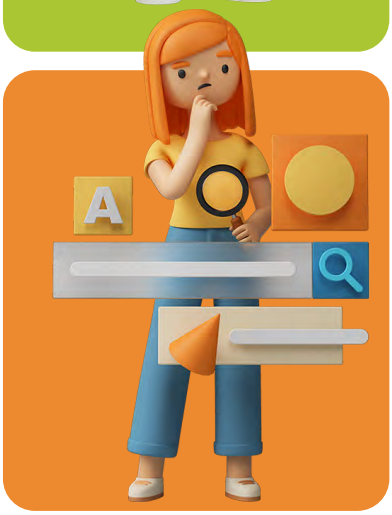
Conozcamos tus resultados

Recuerda que mantenerse informados es la mejor defensa contra los riesgos de una vida digital.
¡Nunca es tarde para ser una familia cibersegura!

12-16 Respuestas afirmativas

Tu hija/hijo esta ciberseguro

¡Increible!, Tus hijas/hijos se encuentran ciberseguros, recuerden no bajar la guardia y mehorar día con día su seguridad y la de tu familia dentro de la vida online.



06-11 Respuestas afirmativas

Falta muy poco

Van muy bien, pero siempre se puede mejorar, tomen en cuenta sus respuestas y manos a la obra con las acciones que faltan, poco a poco pueden estar ciberseguros, recuerda que la información es su mejor defensa.

01-05 Respuestas afirmativas

podemos darles algunos tips

Tranquilos, nunca es tarde para estar ciberseguros, mantenerse al tanto de las herramientas tecnológicas permitirá aprovecharlas a su favor y esta guía puede ayudarlos con esa tarea.

¿A qué edad le compro un teléfono celular a mi hija o hijo y cuál es mi responsabilidad al hacerlo?

Tú decides cuál es la edad correcta para darle a tus hijas o hijos su primer teléfono celular, sin embargo, debes considerar su nivel de madurez, su capacidad de obedecer las reglas del hogar y la escuela, ademas de tomar en cuenta su sentido de la responsabilidad.

Cuando le das un teléfono celular a tus hijas o hijos, les estás dando una **herramienta poderosa para comunicarse y producir contenido,** crear textos, imágenes y vídeos que pueden subir en sitios web al instante y distribuirse por todos lados. Por ello las madres, padres y cuidadores deben considerar si sus NNA están listos para usar un teléfono de manera responsable y respetuosa.

Si piensas que la habilidad de tus hijas o hijos para manejar la tecnología es mayor al nivel de responsabilidad que han demostrado, presta atención a las siguientes preguntas, quizás tengas que decir: "Todavía no es momento."

- ¿Necesitas estar en contacto con tu hijo por motivos de seguridad?
- ¿Tu hijo ha demostrado ser responsable? Por ejemplo, ¿te avisa cuando va a salir de casa? ¿Regresa cuando dice que lo hará?
- ¿Tu hijo se beneficiará de poder estar en contacto más fácilmente con sus amigos?
- ¿Crees que usará el celular de forma responsable; por ejemplo, no enviará mensajes de texto en clase o molestará a otros con sus conversaciones por teléfono?
- ¿Respetará tu hijo los límites que le pongas para usar el celular como la cantidad de minutos para hablar o cuándo y dónde puede usarlo?
- ¿Usará los mensajes, fotos y videos responsablemente y sin avergonzar o molestar a otros?

Tips para la enseñanza y apoyo dentro y fuera del mundo digital

El apoyo que requieren Niñas, Niños y Adolescentes más allá de la experiencia digital, terminarán por facilitar el aprendizaje y entendimiento mutuo para lograr prevenir problemáticas del mundo moderno.

¡Veamos algunos consejos!

Muestra disposición para hablar sobre temas de interés.

Es importante que como madre, padre o cuidador te intereses por la vida digital de tus hijas e hijos, conozcas las nuevas tendencias del mundo digital y reconozcas que aquello que para ti puede no ser tan importante, para tu hija o hijo puede ser un tema vital.

Aprende a confiar

Debemos comprender que conforme las NNA se van desarrollando, buscan mayor autonomía en su vida, por esta razón debemos considerar que si los más pequeños de la casa ya poseen la habilidad para navegar por plataformas, esto es un gran comienzo para fomentar la confianza.

Infórmate e infórmalos

Es importante establecer con las NNA normas sobre cuándo, dónde y cómo utilizar de manera segura los dispositivos, cuidar su privacidad y seguridad, así como hablar contigo u otros adultos de confianza si sufren situaciones que los incomodan en Internet.

Respeta los límites y privacidad

La mayoría de las veces las NNA buscan tener espacio para pasar el rato con sus amigos sin sentirse vigilados, puede resultar difícil asumir que tu hija o hijo no quiere que lo sigas en alguna red social, un diálogo de confianza puede ayudar a tener un mutuo entendimiento y tranquilidad tanto en línea como fuera de ella.

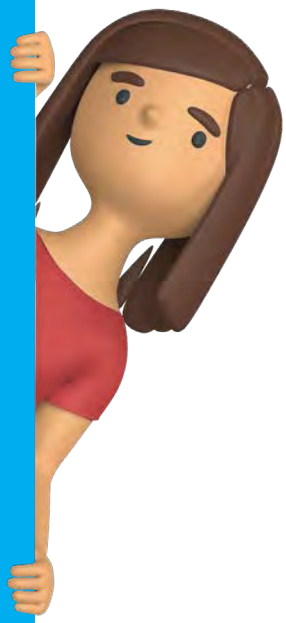
Maneja con tranquilidad las diferentes situaciones que pueden presentarse

Si tu hijo acude a ti en busca de ayuda, debes procurar no reaccionar mal o minimizar la situación, incluso si resulta difícil entender mantén una escucha activa y sin recriminación.

Mantente alerta

Si observas que tu hija o hijo parece preocupado, muestra mal humor, angustia, o depresión, podrían ser signos de que está enfrentando alguna forma de violencia a nivel digital, se debe estar atento a cualquier cambio de comportamiento y si es necesario acercarte a la Policía Cibernética Municipal.

¿Qué hacer cuando mi hija o hijo esta en “cierta edad”?

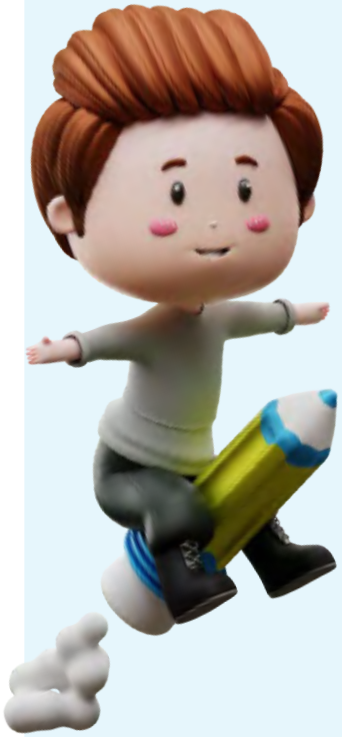


Consejos para afrontar el mundo digital de mi hija o hijo y no morir en el intento.

Sea cual sea la edad puedes aprovechar la tecnología y la información existente para apoyarte, tenemos algunos consejos para diferentes grupos de edad que harán más seguras las actividades en Internet.

¡Dales un vistazo!

De 8 a 10 años



Guía y acompaña a tus hijos en sus primeras eperiencias en la web

Cerciórate de estar presente cuando tus hijas o hijos den sus primeros pasos dentro del mundo digital, **el primer contacto con Internet es una buena oportunidad para sentarse y mostrarles los alcances,** riesgos y bondades en su nueva aventura.

Plantea algunas condiciones para usar internet

Algunas reglas básicas para usar Internet nunca están de más, una buena práctica es **supervisar el número de horas que se pasan conectados y establecer los horarios** en los que se permite el acceso a la red.

Sé el ejemplo perfecto

Las niñas y niños suelen tomar como ejemplo el comportamiento de sus madres y padres, celebridades del momento u algunas otras personalidades de los medios de comunicación, series, películas, entre otros más; **seguir o admirar a personas o personajes que mantengan comportamientos positivos** facilitará que tu hija o hijo siga el ejemplo.

DE 11 A 14 AÑOS

Enséñales a no compartir información

Es de vital importancia dejarle claro a los niños que **dentro del mundo virtual no todos son nuestros amigos y que algunas personas pueden incluso querer dañarlos,** explícales que no es seguro compartir datos como su dirección, números de teléfono, lugar en donde estudia, entre otros datos, e infórmales que es importante algunas veces pedirte autorización antes de compartir fotos potencialmente sensibles en Internet.

Mantén un buen diálogo

Anima a tus hijas o hijos a ser abiertos contigo y a preguntar libremente sobre lo que ven en Internet, **si utiliza una computadora de escritorio, intenta instalarlo en una habitación en la que pase toda la familia y donde pueda estar bajo tu supervisión, no en su dormitorio.**

DE 15 A 18 AÑOS

Uso seguro de videojuegos

Jugar es una de las actividades más habituales de los adolescentes al utilizar las TIC, sin embargo, existen riesgos que van desde las pérdidas económicas hasta el contacto con personas poco deseables, pasando por posibles adicciones o situaciones de aislamiento, por ello, es importante enseñarles a valorar su privacidad, tener cautela al tratar con personas a las que no conocen y establecer normas de uso, contenidos y tiempos.

Denuncia inmediatamente el acoso y el ciberacoso

Hoy en día muchos de los problemas escolares se han trasladado a la tecnología, lo que no ha cambiado es el hecho de intentar dañar psicológicamente a otros, si alguna vez sufren acoso escolar, o lo presencian es importante comunicarlo, así como recordar que situaciones como la creación de memes, stikers o grupos privados, pese a ser tan cotidiano pueden generar acoso.

Las compras online deben hacerse solo con ayuda de un adulto.

Comprar algo en Internet no debería ser un problema, siempre que se haga con cuidado, hasta que los adolescentes comprendan la precaución necesaria al enviar información financiera personal y deben hacerlo únicamente bajo supervisión.

Protégete y protégelos

Consejos de ciberseguridad

Cuando te encuentras navegando por Internet, redes sociales u otras aplicaciones, es importante que te preocupes por implementar mecanismos de seguridad.

Crea una contraseña segura para tu teléfono y aplicaciones.
Usar contraseñas únicas para cada aplicación garantizará que la persona que busque robar tus datos no tenga acceso a tu información.

Mantén tu teléfono bloqueado.
Es importante tener bloqueada tu pantalla de inicio, ya sea por medio de un código de acceso, un patrón, una huella digital o mediante reconocimiento facial.

Ten cuidado con lo que descargas.
Descargar aplicaciones de tiendas oficiales, con comentarios positivos y valoración alta siempre es una opción más segura, evita descargar Apps desde enlaces externos o páginas que puedan ser falsas o apócrifas.

Ten cuidado con lo que publicas.
Recuerda que lo que publiques en Internet no desaparecerá nunca, una fotografía puede ser tomada y editada, cambiando el contexto de la publicación con fines maliciosos.

Apaga la red WiFi y el Bluetooth cuando no los uses.
Cuando mantienes activos el Bluetooth y las redes WiFi, los cibercriminales pueden ver a qué redes te has conectado antes, suplantarlas y engañar a tu teléfono para que se conecte a los dispositivos WiFi y Bluetooth que llevan los usuarios mal intencionados, pudiendo comprometer tu información.

Usa la verificación en dos pasos.
Es imprescindible habilitar esta opción siempre que puedas, la verificación en dos pasos impide que las personas con mala intención inicien sesión en tus cuentas, aunque estas conozcan tu contraseña.

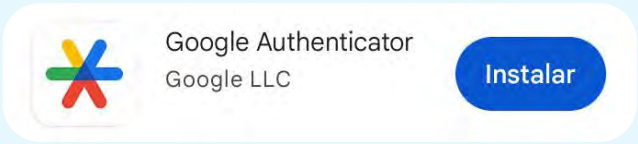
¿Verificación que?...

Verificación en dos pasos, más que una opción, una necesidad.

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 nuestra cuenta o las cuentas de tu familia.

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.

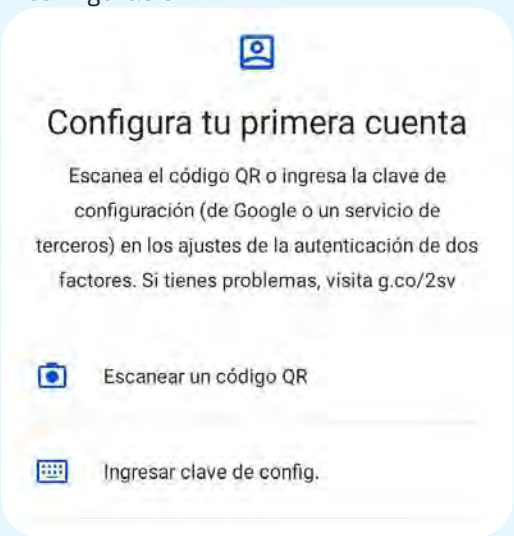
Google Authenticator te permite vincular tus cuentas de Google a la App para que sea más fácil recuperar tu información en caso de perdida o robo.

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, X (antes 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?

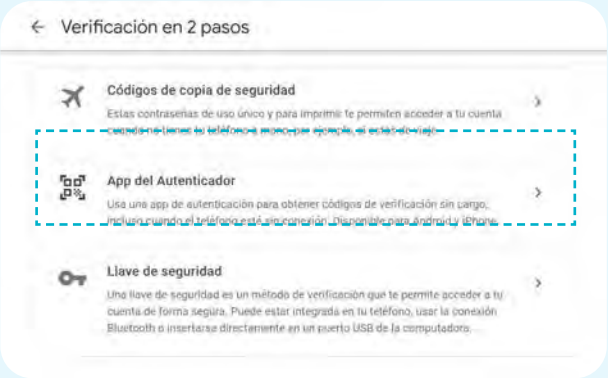
Los pasos a seguir para obtener un código QR varían dependiendo de cada cuenta, sin embargo podemos darte los pasos generales para obtenerlo.

- 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

Riesgos en la red

Los riesgos de la vida digital pueden vulnerar a cualquiera, sin embargo, las NNA pueden encontrarse más susceptibles a ellos.

Conoce los riesgos, ¡la prevención inicia contigo!

Riesgos de contenido

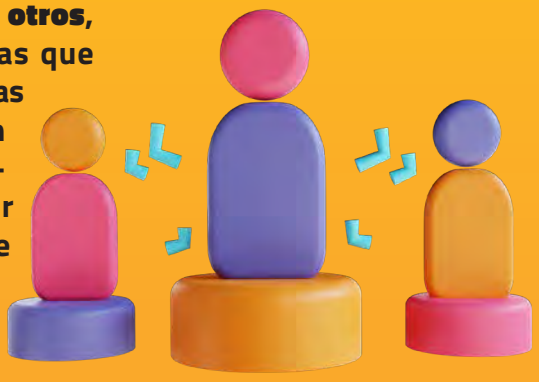
Son riesgos en los que una niña o niño está expuesto a contenidos inapropiados o ilegales, esto puede incluir **imágenes sexualmente explícitas, pornográficas, violentas o inapropiadas para la edad.**

Riesgos de contacto

Son aquellos en los que **una niña o niño interactúa con adultos que buscan contacto inapropiado o con fines sexuales** haciéndose pasar por una persona de su edad, a esto se le conoce como grooming.

Riesgos de conducta

Son aquellos en los que una niña o niño tiene **conductas riesgosas o dañinas para si mismos o para otros,** motivados por las cosas que encuentra en Internet o las personas que expresan puntos de vista extremistas que buscan persuadir a NNA para que participe en comportamientos peligrosos, **¿te suenan los retos virales?**



Las diferentes problemáticas a las que se ven expuestos Niños, Niñas y Adolescentes ya sea a nivel social o digital traen consigo cambios conductuales o físicos que pueden señalar la existencia de alguna problemática.

Debemos estar atentos.

Pon atención a las señales

Las diferentes problemáticas a las que se ven expuestas Niñas, Niños y Adolescentes, ya sea a nivel social o digital traen consigo cambios de conducta o físicos que pueden señalar la existencia de algún problema.

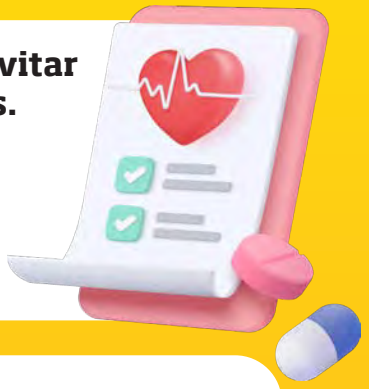
¡Debemos estar atentos!

Somatizaciones diversas

Dolores de cabeza, dolores de estómago, pérdida de apetito, insomnio, malestar generalizado.

Finge dolencias para evitar situaciones y entornos.

Por las mañanas se encuentra mal o dice sentir algún dolor, en la escuela dice que no se encuentra muy bien y pide que le vayan a recoger.



Cambios de hábitos.

No quiere asistir a la escuela, pide que lo acompañen o cambia su ruta habitual, no quiere socializar o salir con amigos, entre otros.

Cambios de carácter.

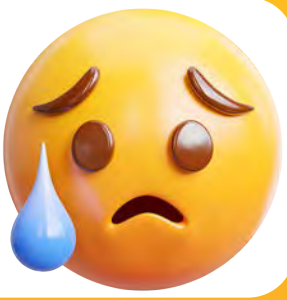
Esta irritable, se aísla, se muestra introvertido, se ve angustiado, pierde confianza, muestra nerviosismo, ansiedad, rabia contenida, crisis de angustia, etc.

Replica la violencia.

Comienza a amenazar y agredir a otros niños o a sus hermanos.

Cuadros depresivos.

Llegando algunos a la actuación o idealización suicida.



Ansiedad.

Cuando los niños tienen miedos y preocupaciones y estos llegan a ser demasiados que interfieren con las actividades escolares, en la casa o en el juego, puede ser diagnosticado un trastorno de ansiedad.

Cambios en la actitud hacia las tareas escolares.

Baja su rendimiento escolar, fobia escolar o social.

2 DELITOS INFORMÁTICOS

¿Cuáles son? ¿Cómo identificarlos?

Medidas y Prevención

Has llegado al capítulo II de esta Guía, aquí encontrarás los delitos informáticos más comunes que vulneran a Niñas, Niños y Adolescentes, sus características, cómo actúan y algunas soluciones para atenderlos, ¡así que sigue adelante!

Entendemos que, de manera casi general, las Niñas, Niños y Adolescentes se encuentran conectados por medio de algún dispositivo y durante grandes cantidades de tiempo, sin llegar a considerar los riesgos que pueden existir dentro de Internet, es por ello que las madres, padres y cuidadores deben contar con la mayor cantidad de información sobre dichos peligros, así como el conocimiento sobre herramientas preventivas que puedan aminorar los riesgos.

¿Te ha pasado?

Te presentamos una serie de preguntas que puedes hacerle a tus hijas e hijos para conocer un poco de su entorno escolar y digital, no existen preguntas mágicas que sirvan para detectar de manera certera una problemática, sin embargo, estas preguntas te permitirán detectar algunas señales para prestar atención.

	SÍ	NO
1. ¿Has notado algún conflicto entre estudiantes de tu clase?		
2. ¿Crees que es frecuente que se usen las nuevas tecnologías y redes sociales para hacer daño a otras personas?		
3. ¿Conoces algún caso en el que un estudiante haya sido o sea agredido o insultado frecuentemente a través de las redes?		
4. ¿Alguna vez has visto a alguien grabar o tomar fotos a otro sin su permiso?		
5. ¿Alguna vez has visto alguna publicación o grupo en Internet en el que se rían de una compañera o compañero?		
6. ¿Alguna vez te ha ocurrido a ti algo similar a lo anterior?		
7. ¿Alguna ocasión te has sentido intimidado en clase o te han amenazado por medio de Internet?		
8. ¿Se lo has contado / contarías a alguien para recibir ayuda o ayudar a otros?		
9. ¿Alguna vez tú has agredido o te has burlado de alguien en Internet?		
10. ¿Piensas que es normal agredir o burlarte de alguien por medio de Internet?		

Revisemos las respuestas

Las situaciones de riesgo en internet suelen ser un proceso sumatorio, que en conjunto a las acciones que puedan ocurrir a nivel personal llegan a incrementar el daño de forma exponencial y de no lograr prevenir pueden generarse graves secuelas psicológicas e incluso físicas

De 01 a 05 respuestas afirmativas
Podemos prevenir

Hazle saber a tu hija o hijo que puede contar contigo y que vas a estar siempre con él para ayudarle en lo que necesite, mantén un estado de observación permanente ante posibles señales que puedan alertar sobre situaciones de riesgo, fomenta el diálogo y el uso sano de la tecnología.

De 06 a 08 respuestas afirmativas
Debes estar alerta

Hazle saber a tu hija o hijo que **los dispositivos móviles al igual que Internet no se deben usar para fomentar comportamientos que vulneren a otros o a sí mismo,** pues se podría estar incursionando en algún delito.

De 09 a 10 respuestas afirmativas
Debes actuar

Anima a tu hija o hijo para que no permita que vuelvan a producirse situaciones que lo vulneren o vulneren a otros dentro y fuera del mundo digital, coméntale que debe informar a su docente sobre la situación que se está presentando e invítalo a hablar contigo siempre que se presente alguna situación similar.

Hablemos de 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 del uso 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

Etapa más vulnerable

Adolescencia 12-17 años.
(Mociba, 2021)

¿Qué es?

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?

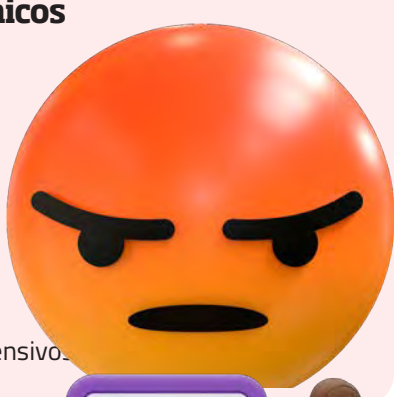
Conoce las diferentes formas:

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.

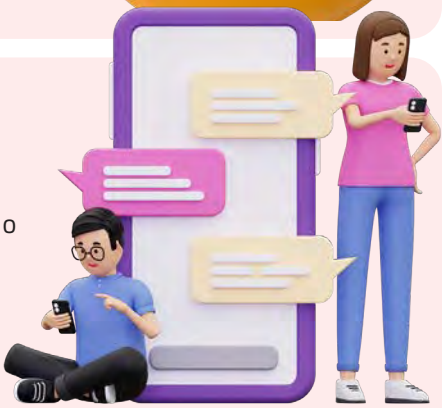
Denigración

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

¿Necesitas reportar el contenido de alguna red social?, te dejamos los enlaces de reporte para que puedas hacerlo de manera rápida.

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

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

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

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

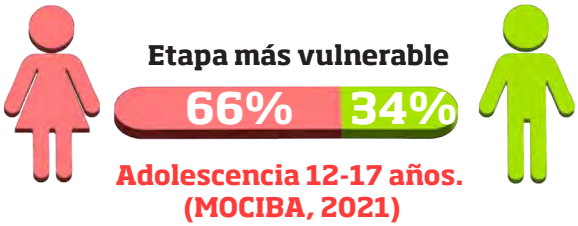
Retirar de google imágenes personales explícitas o íntimas no consentidas.
https://supoort.google.com/websearch/answer/6302812

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

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 una NNA, tanto de manera física como a través de Internet, mediante la interacción y la obtención de material sexual de la niña, niño o adolescente.

¿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 la 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 Niña, Niño o Adolescente.

Acceso y contacto inicial con las NNA.

1

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.

Los agresores adaptan el lenguaje a la jerga típica de las NNA y crean una identidad más deseable acorde a los gustos de las niñas, niños y adolescentes.

Pueden llegar a compartirse números telefónicos o redes sociales con otros usuarios, para después introducirlos a aplicaciones como Telegram o Signal, que permiten un anonimato y dificultan las investigaciones de las Fuerzas del Orden.

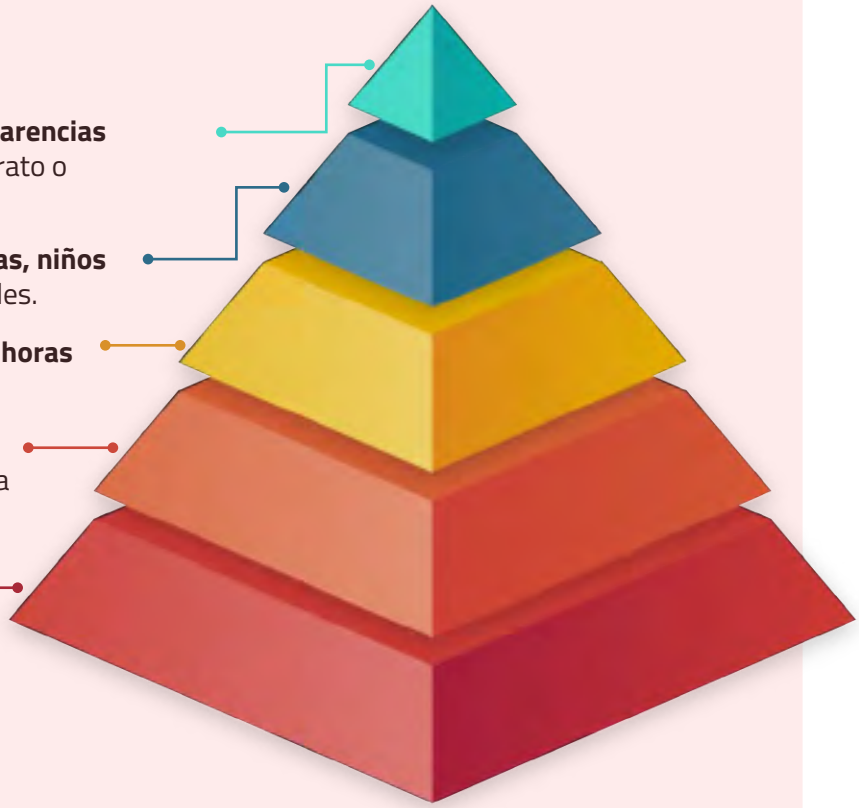
Escenarios que facilitan el contacto inicial

Observar cambios de conducta puede ser un punto de partida para atender alguna problemática que pueda estar suscitándose, debe existir la confianza para compartir el teléfono en cualquier instante.

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.
- Suelen mantener **conversaciones a altas horas de la noche.**
- **Hacen cumplidos a la víctima buscando mayor cercanía,** algunos incluso "juegan a ser novios".
- **Piden que no se comente a nadie** sobre las conversaciones que se tienen.



3 Estrategias de actuación.

Los agresores desarrollan una **serie de estrategias de persuasión que parecen utilizar para adaptarse a las necesidades de las niñas, niños y adolescentes.**

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 2021 en a nivel nacional se registraron 5,375 delitos de extorsión en sus diferentes modalidades, siendo los más afectados hombres. (ENVIPE, 2022)

El secuestro virtual, conocido también como extorsión, 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, no violento, 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.**

¿Qué condiciones posibilitan un secuestro virtual?

Para que el secuestro virtual exista, opere y funcione como una estrategia de despojo, es necesario que se de una condición básica.

Falta de comunicación.

La poca comunicación que puede vivirse dentro de los núcleos familiares facilita que el extorsionador fabrique estrategias que pueden resultar creíbles para las víctimas.

4 Sexting

Enviar fotos o vídeos de contenido sexual

¿Qué es?

Etapa más vulnerable

79% 21%

Adolescencia 11-17 años (MOCIBA, 2021)

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 fotografías y vídeos 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, pública, 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 sin el consentimiento del involucrado, se puede llegar a incurrir en delitos tales como: extorsión, pornografía y prostitución, ya que divulgar este contenido sexual por cualquier medio afecta la vida sexual, privacidad y reputación.

¿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.

Etapa más vulnerable

79% 21%

Adolescencia 11-17 años (MOCIBA, 2021)

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.

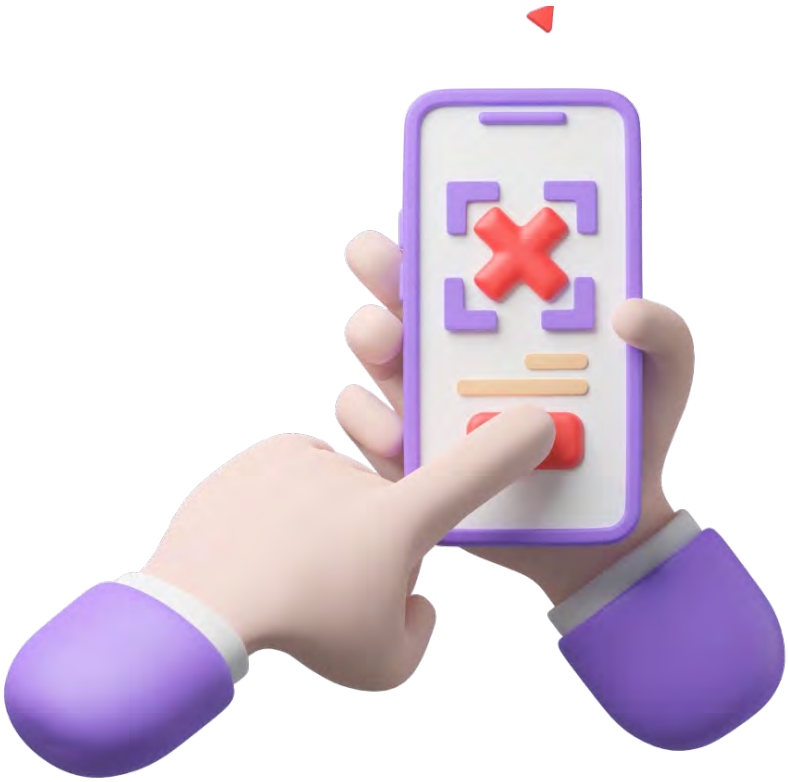
Código Penal del Estado de San Luis Potosí

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.

¿Necesitas reportar el contenido de alguna red social? Consulta los enlaces de reporte de la página 38 para que puedas hacerlo de manera rápida.

Nunca sin mi consentimiento

La alternativa de facebook para evitar la sextorsión

Facebook ha estado probando 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.

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

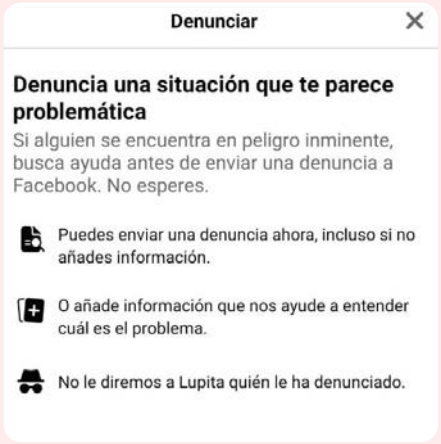
En Facebook, Instagram o Messenger, puedes denunciar que una persona haya compartido imágenes íntimas sin tu consentimiento o te haya amenazado con hacerlo.

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.

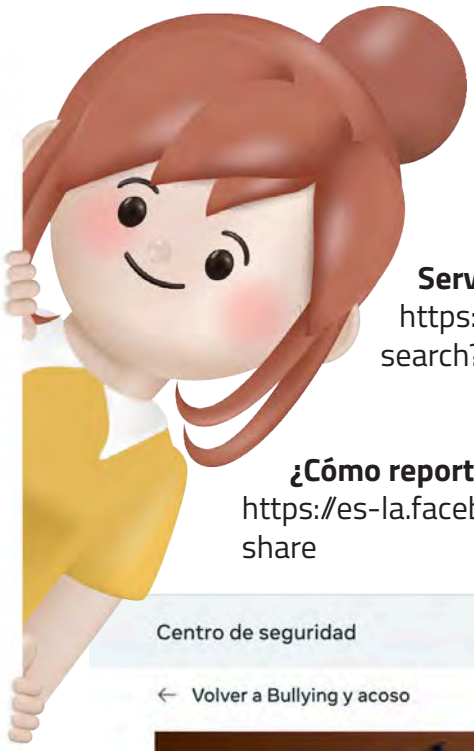


4 **Selecciona la opción** que mejor describa el problema y sigue las instrucciones que aparecen en pantalla.

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?

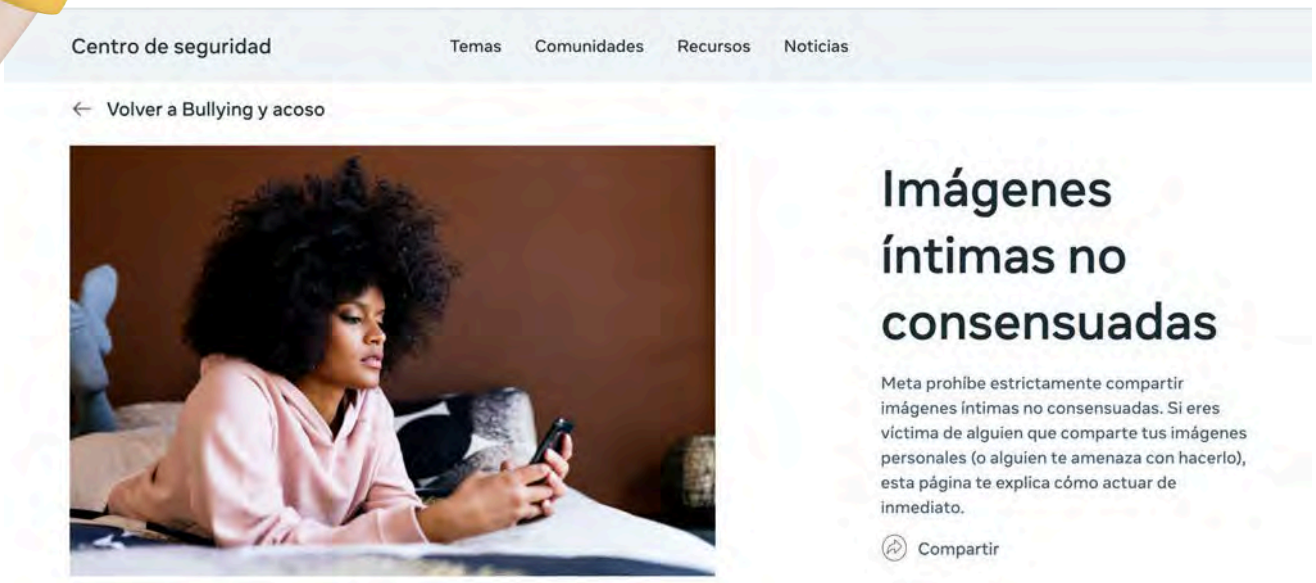
¡Echa un vistazo a los siguientes enlaces!



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?

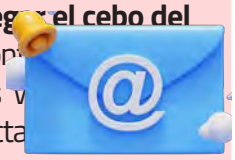
El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robar tu información privada, hacer algún cargo económico o infectar tu dispositivo, 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 suelen con enlaces que llevan hasta sitios v maliciosos o archivos adjuntos infecta 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.

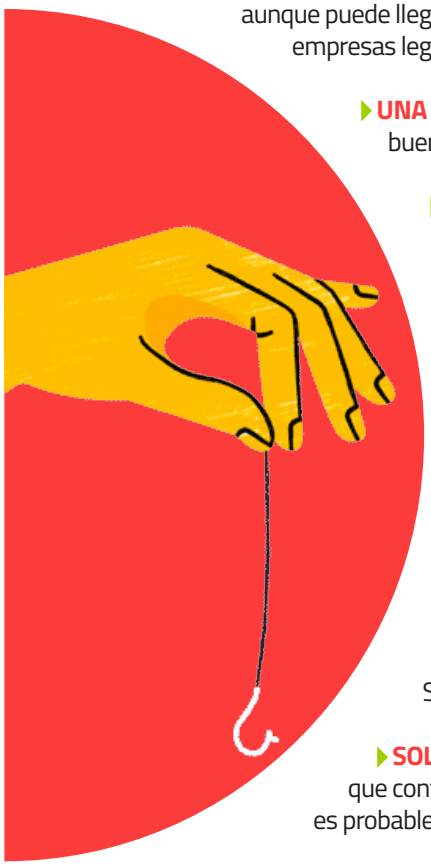
SMISHING

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. Muchas robollamadas son intentos de vishing.

¿Qué aspecto tiene un correo electrónico/ mensaje/llamada de phishing?



- **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.

Herramienta digital

La identificación de un ataque de suplantación de identidad (phishing) puede ser más difícil de lo que piensas, **Jigsaw, la incubadora tecnológica de Google, lanzó una herramienta interactiva que pone aprueba tu habilidad para identificar ataques de phishing por medio de un juego.**

¿Podrías detectar qué es falso?

https://phishingquiz.withgoogle.com/?hl=es

8 Violencia Online

En la pareja o ex pareja

¿Qué es?

ETAPA MÁS VULNERABLE

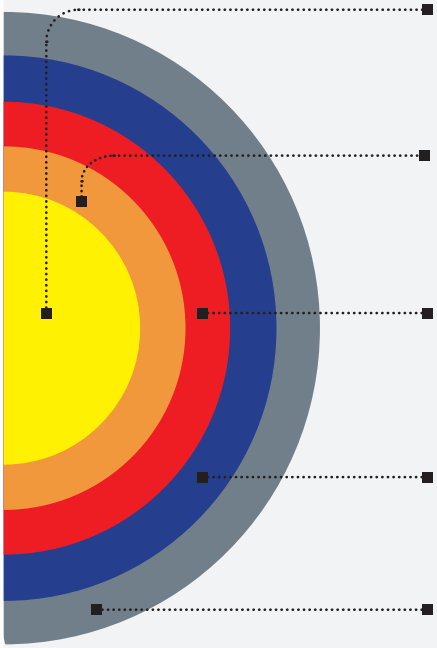
63% 37%

ADOLESCENCIA 12-17 AÑOS.
(OMS, 2016)

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.

Indicadores de la violencia digital en la pareja

Como madre, padre y cuidador, es de utilidad auxiliar a tu hija o hijo a salir de una relación tóxica que pueda vulnerarla o vulnerarlo.



- 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

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 de personas desnudas o manteniendo relaciones 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.

Incitación a conductas dañinas.

Niñas, niños y adolescentes 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.

Sharenting, la sobreexposición de menores en internet.

Aunque este no es un tipo de violencia, si se considera como una actividad de riesgo.

Share = Compartir
Parenting = Crianza

Es la práctica cada vez más habitual de madres, padres y cuidadores en la que exponen pública y constantemente la vida de sus hijas e hijos en la red, en principio, puede parecer una costumbre inofensiva, pero debemos ser conscientes de las consecuencias que puede tener para las vidas de niñas, niños y adolescentes.

Recordemos en dónde puedes reportar contenido

¿Necesitas reportar el contenido de alguna red social?, te dejamos los enlaces de reporte para que puedas hacerlo de manera rápida.

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

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

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

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

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

10 Algunas páginas y Apps de riesgo, ¿Tu hija o hijo las usa?

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 los estudiantes se exponen 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 son?

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, X (antes 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?

Estas plataformas **están diseñadas para ser usadas por adultos,** no niñas o niños, riesgos como depredadores, desinformación y fugas de datos, hacen de estas plataformas un sitio nada seguro para niñas, niños o adolescentes.

No son seguras para nadie menor de 15 años, incluso entonces, querrás considerar la madurez de tu hija o hijo y cómo respondería si encuentra contenido para adultos, incluso con los moderadores de contenidos y las funciones de seguridad, la probabilidad de que tu hija o hijo se tope con algo inapropiado es alta.

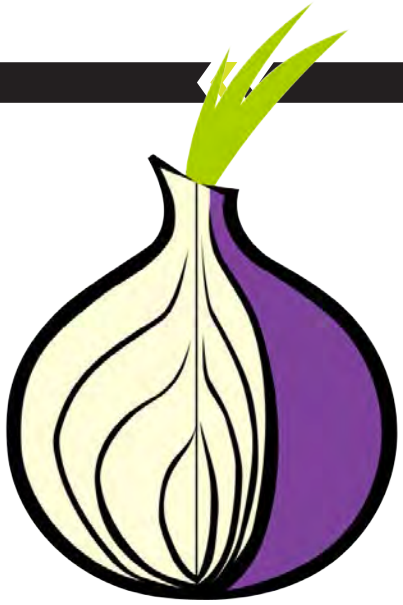
¿Cuáles son los riesgos de usar estas plataformas?

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 gratis y de fuente abierta creadas para cualquier usuario de Internet que busque mantenerse anónimo y obtener seguridad extra en línea. Están diseñadas para detener al gobierno de acceder a tus registros, monitorear tus hábitos de navegación, y tu información personal, hacen que sea difícil rastrear la actividad del usuario.

¿Es seguro su uso?

Si bien, estos navegadores ayuda a proteger la anonimidad del usuario, su uso por parte de NNA puede ser un riesgo o un beneficio esto depende de cómo las niñas, niños y adolescentes lo utilizan ademas de su entendimiento sobre este tipo de navegadores.

Intentar protegerlos a traves de estos medios podría significar exponerlos a algunos peligros inevitables, por lo que resulta necesario monitorearlos y educarlos sobre el uso de estos navegadores, así como brindar información sobre algunos sitios web (especialmente sitios .onion) que no deberían visitar.

¿Cuáles son los riesgos de usar estos navegadores?

Estos navegadores exponen a las desventajas de la web oscura, donde se llevan a cabo actividades ilegales, tales como el robo de datos sensibles, compra de contrabando, tratos de drogas, pornografía infantil y otras similares, esto es particularmente peligroso si tus hijas o hijos están involucrados. El uso obsesivo de estos navegadores los puede llevar a encuentros directos con criminales y personas con motivos peligrosos.

Algunos criminales pueden agregar malware a un nodo existente de la red, robando tu información.

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.

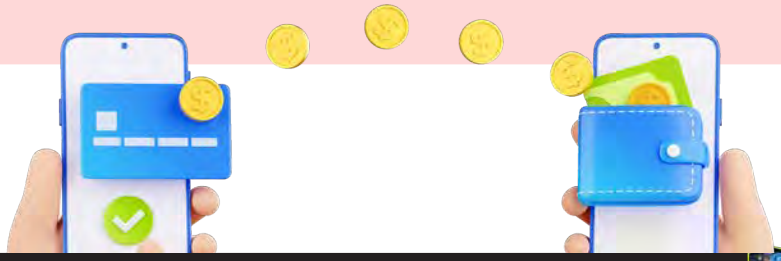
¿Es seguro su uso?

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.**



Ya conozco los riesgos... ¿Ahora que hago?

Te presentamos unos **consejos que te serán de utilidad para prevenir y actuar ante situaciones de riesgo en Internet,** de igual manera recuerda que la Policía Cibernética del Municipio de San Luis Potosí esta a tu servicio siempre que la necesites.

Inicia un diálogo positivo e identifica la problemática

Si de manera inicial logras identificar alguna señal que pueda decirte que tu hija o hijo se encuentra pasando por alguna problemática, lo recomendable es promover el diálogo empático sin minimizar sus pensamientos y sentimientos, una vez teniendo conocimiento de la problemática debes hacerle saber que es posible llegar a una solución de manera conjunta.

Recuérdale la importancia de las contraseñas, de mantener la información y material online privado.

Siempre es importante recordar la importancia de mantener nuestra información segura, si existe algún riesgo de que puedan ingresar a la cuenta de tu hija o hijo, cambia inmediatamente las contraseñas de sus cuentas, también es recomendable cambiar la privacidad de sus redes sociales para que su información no sea visible para todo el mundo.

Usen la tecnología a su favor.

Cada plataforma y red social cuenta con herramientas que pueden apoyarnos para detener alguna situación de ciberbullying, happy slaping, grooming, entre otras, por lo que es importante conocerlas y usarlas a nuestro favor, podemos bloquear a algún usuario problemático, poner privadas nuestras cuentas, reportar alguna publicación, denunciar o reportar a algún usuario, etc.

Ve siempre un paso adelante y ¡guarda todo!

Debemos tomar en cuenta que guardar evidencia de la problemática es un punto fundamental que nos ayudará a tener un sustento sobre los hechos sucedidos.

La forma en que se puede respaldar la información es por medio de:

- Almacenar capturas de pantalla.
- Almacenar links de páginas.
- Almacenar Fotos.
- Almacenar Comentarios.

Los que terminarán siendo de utilidad en caso de que sea borrada la información o de requerir para futuras denuncias.

Habla con las autoridades pertinentes.

Muchas veces, cuando es visualizado un problema, acudir a la institución educativa de tu hija o hijo para buscar soluciones por medio del diálogo y un acuerdo mutuo, sin embargo, en algunos casos el problema puede no involucrar a sus compañeros de escuela o bien acudir a la escuela no terminó con la situación; en estos casos acudir a instituciones de seguridad que puedan asesorarte es de suma importancia.

La Jefatura de Policía Cibernética de la Secretaria de Seguridad y Protección Ciudadana del Municipio de San Luis Potosí podrá brindarte asesoría y opciones para solucionar la problemática, brindará un seguimiento a la situación, coordinará la atención con las instituciones que sean necesarias, además de brindarte información y proporcionarte el acompañamiento necesario para realizar la denuncia pertinente ante la Fiscalía.

¿Deseas contactarnos?, ¡Adelante!
Te dejamos nuestros datos y esperamos tu llamada.

POLICÍA CIBERNÉTICA MUNICIPAL
Número de Atención/WhatsApp: 444 329 32 81
Facebook: Policía Cibernética Municipal SSPC SLP.

¿Presentarás una denuncia? Te diremos cómo hacerlo

1 ¿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.

2 Localiza dónde denunciar

Para realizar una denuncia puedes hacerlo de tres maneras:

- Acudiendo personalmente ante la Fiscalía del Estado.
- De manera virtual en la página oficial de la Fiscalía del Estado. https://fiscaliaslp.gob.mx/vi/denuncia_virtual/
- De manera telefónica al al 911 o a la Fiscalía General de la República al 800-00-85-400.

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 del Municipio de San Luis Potosí puede brindarte asesoría para realizar tu denuncia, informarte y acompañarte al lugar que debes acudir, comunícate.

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?, de la forma más específica posible.**
- **¿En qué fecha y hora ocurrió?**
- **¿Cuál fue el móvil que motivó el delito?**

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, **solicita 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 las siguientes instituciones:

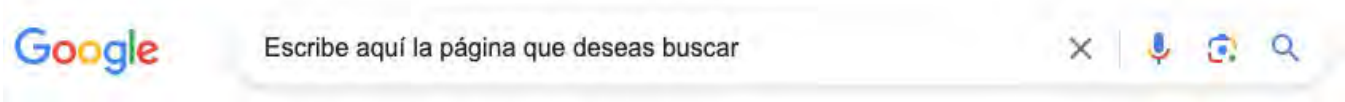
- **Comisión Nacional de Derechos Humanos.**
- **Visitaduría de la Fiscalía.**

¿Cómo guardo las pruebas?

Es importante que recabes toda la información que te sea posible sobre el hecho, en este caso al ser un delito informático, podrás contar con conversaciones, imágenes, videos, paginas web, URL, que podrás presentar al momento de realizar tu denuncia.

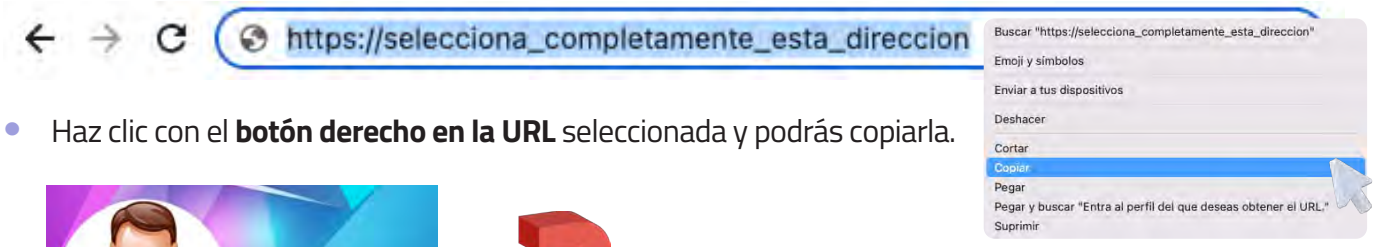
1 Para obtener un URL desde tu computadora

- 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.



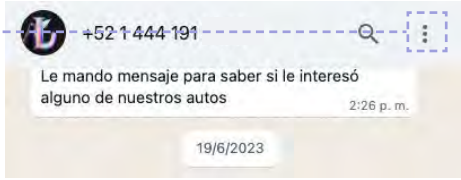
- Haz clic con el **botón derecho en la URL** seleccionada y podrás copiarla.

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

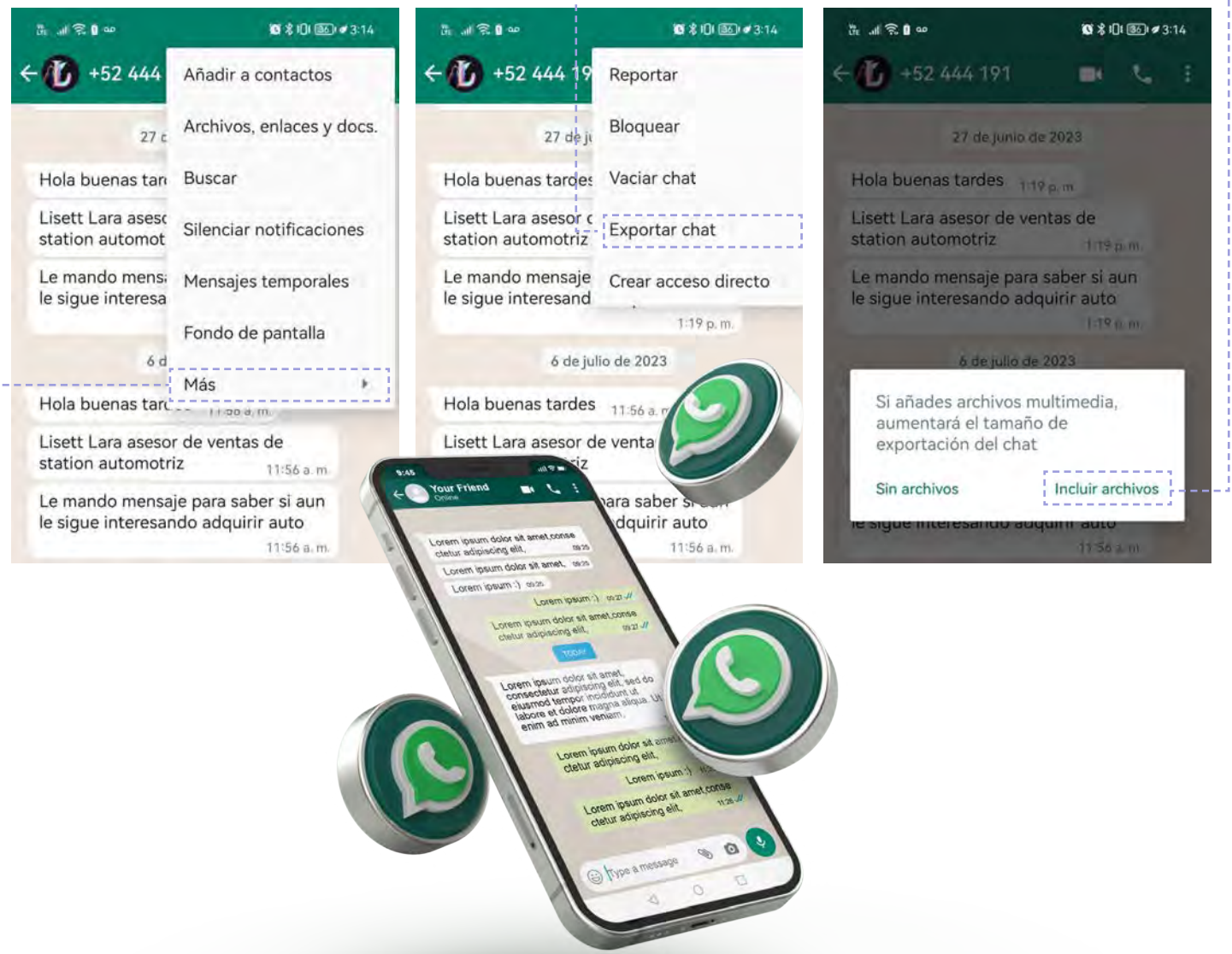
- Entra al perfil del que deseas obtener el URL.
- En el perfil, pulsa los tres puntos que se ubican junto al botón de "Te gusta" (si es una página) o "Enviar mensaje" (si es un perfil).
- Pulsa la opción de copiar enlace.

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 Guia, dentro de esta sección podrás encontrar diferentes herramientas y formas de configuración de controles parentales para tus dispositivos y los dispositivos de tu familia, estas herramientas facilitarán el filtrado de contenidos, el control del tiempo, la supervisión de actividades, la geolocalización y protección de la configuración.

Sin embargo, debes recordar que estas aplicaciones son un complemento en la labor de mediación parental y siempre deben ir acompañadas de actividades digitales en familia que faciliten un clima de comunicación y confianza.

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

Cierto o falso sobre los controles parentales

Vamos a jugar a cierto o falso y veamos que tanto conoces

Selecciona  Si opinas que la oración es cierta.

Selecciona  Si opinas que la oración es falsa.

1. Las herramientas de control parental son software que permite a las madres, padres y cuidadores administrar el uso que hacen NNA de uno o varios dispositivos electrónicos.

2. Las herramientas de control parental solo se pueden usar en teléfonos celulares.

3. Las herramientas de control parental solo sirven para limitar el uso en Internet de las Niñas, Niños y Adolescentes.

4. El uso de controles parentales puede ayudar a monitorear y registrar la actividad online, analizar a donde entra y qué ve tu hija o hijo.

5. Las herramientas de control parental son complicadas de usar.

6. Estas herramientas son una alternativa para tener en cuenta antes de prohibir el uso o el acceso a Internet.

7. Las herramientas de control parental no se deben usar para vulnerar la intimidad de mi hija o hijo.

8. Las herramientas de control parental se deben usar para estar seguro en línea.

Conozcamos las respuestas

1. **Las herramientas de control parental son software que permite a las madres, padres y cuidadores administrar el uso que hacen las NNA de uno o varios dispositivos electrónicos.**
   El control parental es un software que permite generar un entorno digital seguro para NNA.

2. **Las herramientas de control parental solo se pueden usar en teléfonos celulares.**
   El control parental no se limita únicamente a celulares, puede implementarse en cualquier dispositivo que lo permita, por ejemplo, televisores inteligentes y videojuegos.

3. **Las herramientas de control parental solo sirven para limitar el uso en Internet de las Niñas, Niños y Adolescentes.**
   Ademas de limitar el uso de Internet, permite localizar a nuestros pequeños, saber cuanto tiempo pasa en cada aplicación, activar botones de emergencia, entre otras características.

4. **El uso de controles parentales puede ayudar a monitorizar y registrar la actividad online, analizar a donde entra y qué ve tu hija o hijo.**
   El control parental puede crear informes sobre la actividad online de tu hija o hijo.

5. **Las herramientas de control parental son algo complicadas de usar.**
   No necesitas ser un conocedor de la tecnología para usar el control parental, ya que puede ser muy sencillo de utilizar, ademas nosotros te vamos a ayudar.

6. **Estas herramientas son una alternativa para tener en cuenta antes de prohibir el uso o el acceso a Internet.**
   Antes de prohibir a tu hija o hijo usar Internet, estas herramientas pueden ayudarte a considerar los beneficios de navegar por la red y emplear dispositivos tecnologicos, disminuyendo considerablemente los riesgos.

7. **Las herramientas de control parental no se deben usar para vulnerar la intimidad de mi hija o hijo.**
   Usar herramientas de control parental debe ser para generar un ambiente digital seguro, no para vulnerar ni espiar a tu hija o hijo, se debe mantener la privacidad con un pequeño apoyo de seguridad.

8. **Las herramientas de control parental se deben usar para estar seguro en línea.**
   Las herramientas de control parental son los aliados perfectos a la hora de proteger a los más pequeños de la casa, úsala como tu mejor apoyo.

Control parental en cinco minutos o menos

¡Únete al reto!

Las herramientas de control parental **son softwares que permiten a las madres, padres y cuidadores administrar el uso que hacen las NNA de uno o varios dispositivos electrónicos,** además de ser un apoyo en el aprendizaje digital, limitando las funciones y el alcance de sus dispositivos cuando se conectan a Internet, esto incluye desde móviles, consolas o hasta aplicaciones como Netflix.

¿Cuáles son las funciones de las herramientas de control parental?

Existen diferentes funciones para cada necesidad:

1. **Supervisión de actividad:**
Genera informes con el historial de navegación, búsquedas o reproducción multimedia.

2. **Control de tiempo:**
Emite alertas o interrumpe la navegación al alcanzar cierta hora o límite de tiempo.

3. **Filtrado de contenidos:**
Mediante diferentes sistemas, bloquea el acceso del menor a ciertos contenidos inapropiados (habitualmente de connotación sexual o violenta).

4. **Protección de la configuración:**
Evita modificaciones no deseadas de los ajustes de control parental.

5. **Geolocalización:**
Sigue la posición actual y el recorrido anterior del dispositivo.

Ahora conozcamos las diferentes herramientas de control parental, ¡adelante!

Google Family Link

Esta herramienta gratuita de Google para móviles con sistema Android te permitirá **gestionar la actividad de tu hija o hijo en su dispositivo móvil,** además de supervisarle y protegerle de los riesgos asociados a un uso no recomendado.

¿Qué te permite la App?

Filtrar Contenido:
Permite restringir las aplicaciones aprobando o bloqueando las que quiera descargar de Google Play Store.

Controlar tiempo de uso:
Puedes establecer límites de tiempo diarios y configurar una hora de dormir en el dispositivo.

Supervisar:
Te permitirá consultar cuánto tiempo usa cada aplicación mediante informes de actividad semanales o mensuales.

Protección de la configuración:
Permite restringir la modificación de los ajustes de control parental en el sistema Android.

Geolocalización:
Puede permitirte ver la ubicación del dispositivo móvil de tu hija o hijo en caso de ser necesario.

¿Cómo usar la aplicación?

Primer paso
Para comenzar a usar la aplicación será necesario contar con una cuenta de Google, en caso de no contar con una, será necesario crearla, ya que sin esta no podrás usar la app.

Segundo paso
Será necesaria la instalación de la app en tu dispositivo móvil, una vez instalada vincúlate con tu cuenta de usuario de Google.

Si deseas descargarla puedes escanear el QR o ingresar al siguiente enlace:
https://play.google.com/store/apps/details?id=com.google.android.apps.kids.familylink&hl=es_MX

Tercer paso

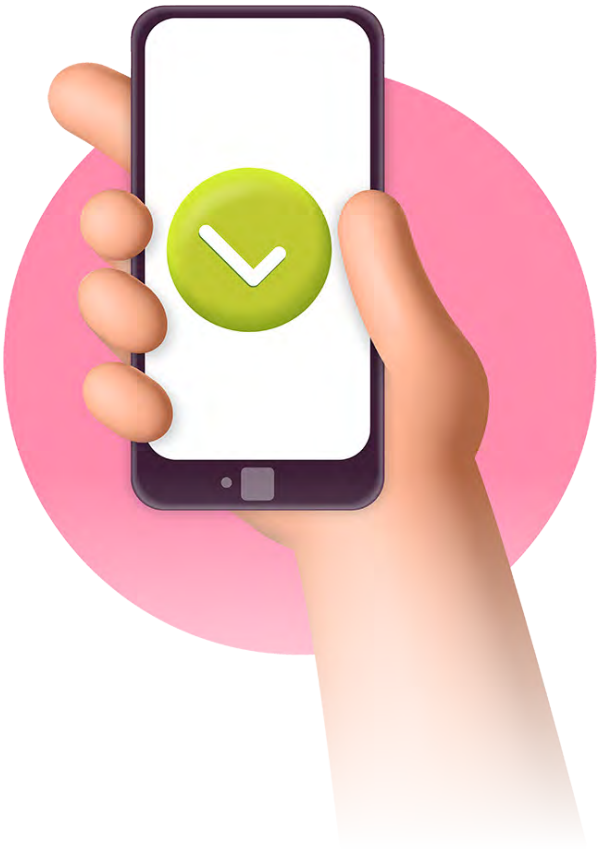
A continuación, crea el perfil de tu hija o hijo. Si no tiene una cuenta de usuario de Google, sigue las instrucciones que aparecen en pantalla y crea una cuenta de usuario.

Cuarto paso

Una vez hayas finalizado la creación de la cuenta, en el dispositivo Android que vaya a utilizar tu hija o hijo, instala la app dirigida a NNA.

Quinto paso

Enseguida introduce el código de configuración para conectar tu dispositivo y el dispositivo de tu hija o hijo.



Sexto paso

Confirma la cuenta de tu hija o hijo.

Séptimo paso

Una vez se hayan sincronizado ambos dispositivos, finaliza la configuración de los requisitos de acceso y filtrado de contenidos del dispositivo dla NNA.

Deseas conocer mas sobre esta App, ¡adelante!, te dejamos un link en el que puedes consultar la página oficial de la aplicación.

https://families.google/intl/es_ALL/familylink/faq/

Aplicación Family Time

Esta apiicación para dispositivos móviles Android e iOS te puede permitir mantenerte informado sobre la ubicación de tus hijas o hijos, podrás administrar el tiempo que pasan en el teléfono, bloquear algunas aplicaciones que no sean adecuadas, entre otras funcionalidades, parcialmente gratuitas.

¿Qué te permite la App?

Filtrar Contenido:
Permite restringir las páginas web accesibles desde el dispositivo dla NNA.

Controlar tiempo de uso:
Ofrece la opción de establecer un límite máximo diario por aplicación.

Supervisar:
Permite acceder a un monitor de actividad digital, donde controlar las apps instaladas, los contactos, los mensajes recibidos y enviados, y los datos navegación.

Bloqueo de aplicaciones y dispositivos:
Permite restringir las páginas web accesibles desde el dispositivo dla NNA.

Geolocalización:
Permite definir zonas de seguridad o de riesgo, y recibir notificaciones al llegar a una zona determinada, ofrece la 'Alerta SOS'.

Control multidispositivo:
Podrás supervisar varios dispositivos desde tu cuenta.

¿Cómo usar la aplicación?

Primer paso
Descargar e instalar la app de gestión FamilyTime en tus dispositivos para facilitar la administración de los controles parentales.

Segundo paso
Como madre, padre o cuidador, deberás crearte una cuenta de usuario para gestionar la cuenta de tus hija o hijo.

Tercer paso
Instala FamilyTime Jr. en el dispositivo de tu NNA, y comienza a configurar los controles.

Si deseas descargarla puedes escanear el QR o ingresa a: **https://play.google.com/store/apps/details?id=io.familytime.dashboard&hl=es_MX**

Aplicación Securekids

Con SecureKids puedes realizar muchas tareas de prevención sobre los dispositivos de las NNA, tales como, permitir o bloquear aplicaciones del móvil, filtrar contenido de internet, como por ejemplo contenido sexualmente explícito, activar búsquedas seguras, o conocer la información de uso del móvil o la tablet.

¿Qué te permite la App?

Llamadas:
Permite el bloqueo o desbloqueo de los números de la agenda y bloquear llamadas de números desconocidos o internacionales para más seguridad.

Descansos:
Es un control de tiempo que permite bloqueos del dispositivo por horas y días.

Geolocalización:
Localización precisa del dispositivo.

Estadísticas:
Permite recopilar información sobre el uso que se está haciendo del dispositivo, y aplicaciones más utilizadas.

Emergencias:
Permite establecer un widget, a modo botón de alarma, que indicará la posición del menor en ese momento y enviará una imagen tomada por la cámara de forma automática.

Alarmas:
Esta función te permitirá establecer alarmas programadas y alarmas instantáneas que se enviarán a tu dispositivo.

Internet:
Esta función te permite controlar las páginas web a las que se puede acceder, bien sea activando la opción 'Listas blancas' de webs permitidas, o utilizando filtros web por categorías, además de permitir activar búsquedas seguras en Google.

Aplicaciones:
Te permite establecer qué aplicaciones puede utilizar el menor, y cuándo podrán ejecutarse en el dispositivo.

Control multidispositivo:
Se pueden agregar a la cuenta varios menores y varios dispositivos para cada menor.

¿Cómo usar la aplicación?

Primer paso
Contar con un dispositivo con sistema Android, Descargar e instalar Securekids en los dispositivos que se quieran monitorizar, tus dispositivos y el de tus hijas o hijos.

Segundo paso
Crear una cuenta de usuario para la app.

Tercer paso
Configurar la cuenta con las opciones de control parental que se deseen, podrás seleccionar las opciones que más se acomoden a tus necesidades.

Si deseas descargarla puedes escanear el QR o ingresa a: **https://play.google.com/store/apps/details?id=io.familytime.dashboard&hl=es_MX**

Aplicación Life360

Life360 es una app de control parental con el objetivo de cuidar a la familia y brindar una solución integral y fácil de usar para todos los seres queridos en un entorno integrado y moderno. El localizador familiar Life360 permite tener conocimiento de la ubicación de todos los miembros de la familia en tiempo real y con una precisión excelente.

¿Qué te permite la App?

Localización Familiar:
Gracias a la tecnología GPS, con esta app disfrutarás de un servicio preciso de ubicación y seguimiento de los dispositivos registrados de tu familia.

Espacios de conexión:
Podrás crear un espacio para que tu familia siempre esté conectada, además de garantizar la seguridad y protección de sus miembros gracias a las funciones inteligentes que ofrece esta aplicación.

Notificaciones:
Podrás recibir al instante notificaciones automáticas cuando los familiares que estén conectados a través de ella vayan a la escuela, al trabajo, regresen al hogar, se desvíen de su ruta habitual y mucho más.

Botón de pánico:
La app pone a disposición de sus usuarios un botón que alertará sobre alguna emergencia, también con la posibilidad de comunicarse con el servicio de emergencia nacional de tu localidad.

Rastrear si el teléfono ha sido extraviado o robado:
Gracias al historial de ubicaciones, es posible establecer una ruta de recorrido que permita rastrear algún dispositivo que haya sido perdido o robado.

Tiempo real:
Podrás compartir la ubicación en tiempo real con tus amigos y familiares que también la estén usando.

¿Cómo usar la aplicación?

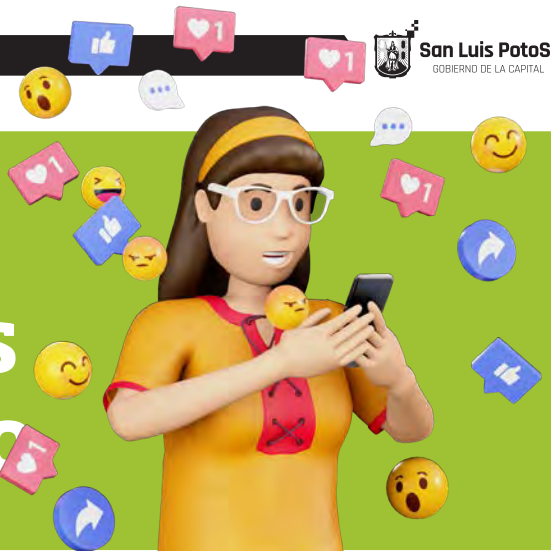
Primer paso
Descarga e instala la app desde la App Store o desde la Google Play Store. Es importante que todas las personas que pretendas incluir en tus Círculos Life360 tengan la app en sus dispositivos.

Segundo paso
Configurartus datos en la app, para ello, debes introducir tu número telefónico donde corresponde y pulsar en «siguiente» para continuar, es importante que ingreses correctamente el número de teléfono, incluyendo el código del país.

Tercer paso
Ingresa una cuenta de correo electrónico que se asociará automáticamente con la app, pulsa en «siguiente» para que continúe el proceso de configuración.

Si deseas descargarla puedes escanear el QR o ingresa a: **https://play.google.com/store/apps/details?id=io.familytime.dashboard&hl=es_MX**

Control parental en redes sociales y Políticas de uso



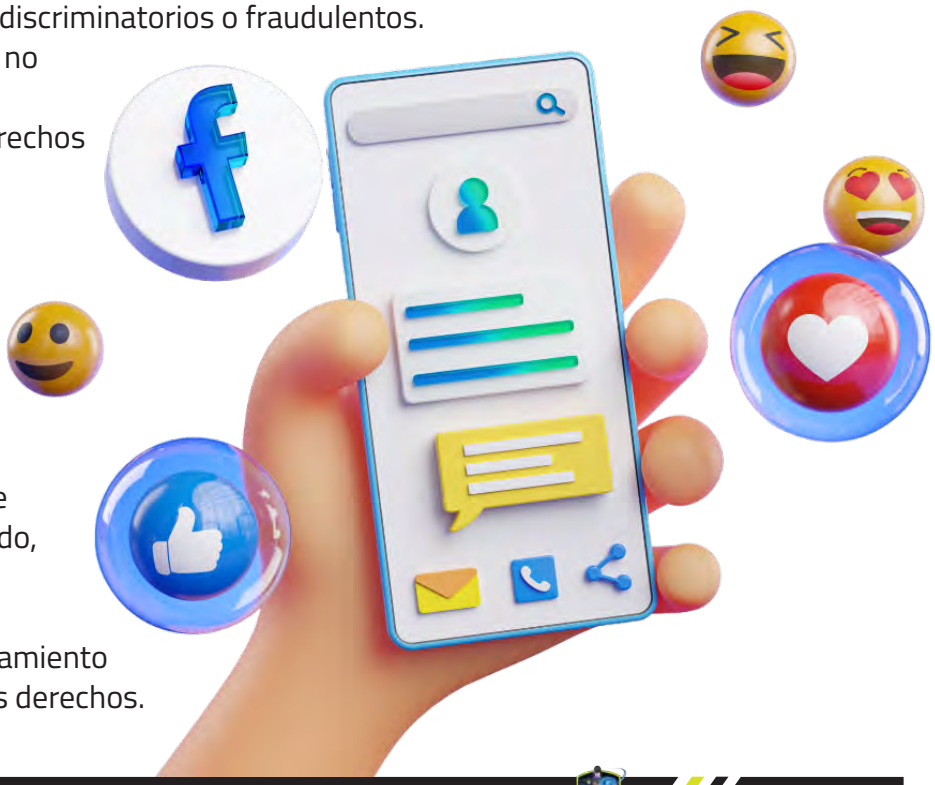
FACEBOOK

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

¿QUÉ PUEDES Y QUE NO PUEDES HACER?

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

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

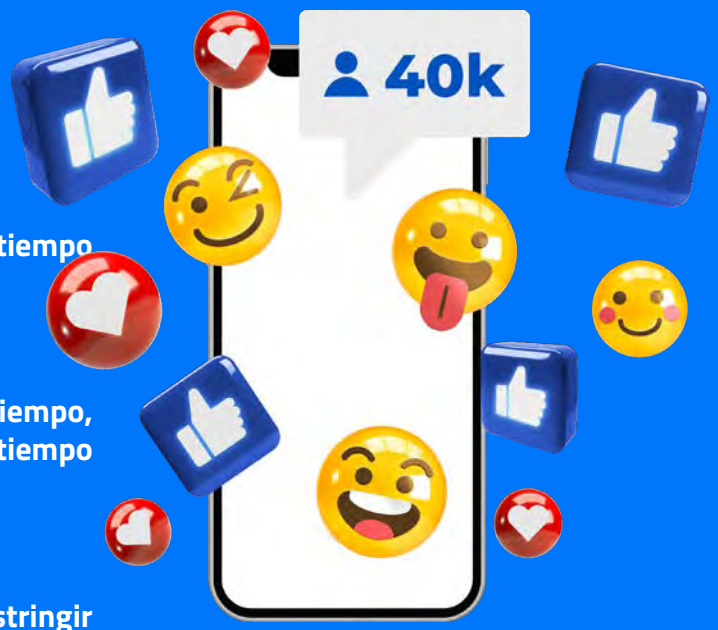
- Violencia: no puedes hacer amenazas violentas contra una persona o un grupo de personas.
- No puedes amenazar o fomentar el terrorismo o el extremismo violento.
- No puedes participar en situaciones de acoso dirigidas a una persona o incitar a otros a hacerlo.
- No puedes fomentar ni promover el suicidio 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.

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

FACEBOOK

Facebook incorpora opciones de bienestar digital, que podemos configurar y revisar para conocer más acerca de la actividad que realiza nuestro hija o hijo en la red social.

¿Qué te permite hacer la App?



- **Seguimiento:**
  La aplicación crea un informe diario indicando el tiempo empleado en la red social.
- **Límite de tiempo:**
  Podemos configurar un recordatorio diario de tiempo, que avisará a la NNA cuando haya superado el tiempo establecido.
- **Filtrado de contenidos:**
  Es posible configurar que la cuenta sea privada, restringir los comentarios de personas desconocidas fuera de su lista de contactos o bloquear comentarios.

¿Cómo podemos configurar el Filtrado de Contenidos?

1

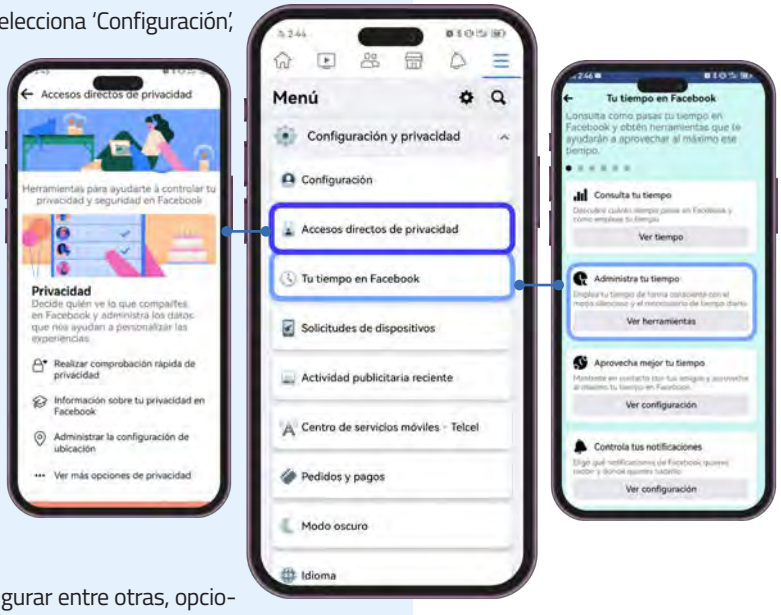
En el menú que se muestra, selecciona 'Configuración', haciendo clic en el icono de tres líneas (ícono hamburguesa) de la parte superior o inferior. A continuación, haz clic en 'Privacidad'.

2

Utilizas Android, dentro del apartado 'Privacidad', selecciona 'Publicaciones públicas'. Si utilizas iOS, desde 'Audiencia y visibilidad' accede a 'Seguidores y contenido público'.

3

En este apartado podrás configurar entre otras, opciones sobre quién puede seguirte, comentar en tus publicaciones, así como clasificar los comentarios.



¿Cómo podemos configurar el Recordatorio de Tiempo?

1

En el menú de configuración, haciendo clic en el ícono de tres líneas en la parte superior, selecciona 'Tu tiempo en Facebook'.

2

Entra en 'Programar recordatorio diario' y ajusta el límite de tiempo. Haz clic en 'Programar recordatorio'.

INSTAGRAM

La red social ofrece algunas opciones de bienestar digital que pueden mejorar la seguridad del menor y ayudarle a hacer un uso adecuado de la App.

¿Qué te permite hacer la App?

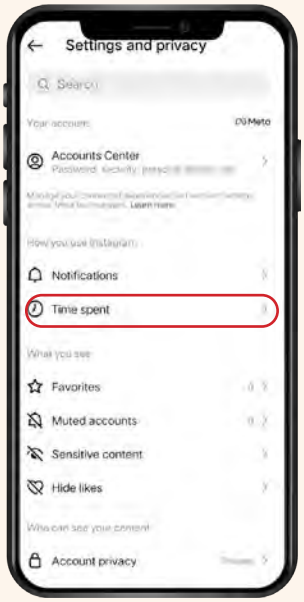
- **Supervisión de actividad:**
  La aplicación recoge todos los datos de uso en la red social, como las solicitudes de amistad, los inicios de sesión, el historial de búsqueda o la interacción con otros usuarios.

- **Límite de tiempo:**
  Puedes programar un recordatorio diario de tiempo, que indique a tu hija o hijo cuándo debe cerrar la aplicación.

- **Filtrado de contenidos:**
  Es posible configurar la cuenta para que sea privada, restringir los comentarios de personas desconocidas o bloquear aquellos comentarios que contengan palabras concretas.

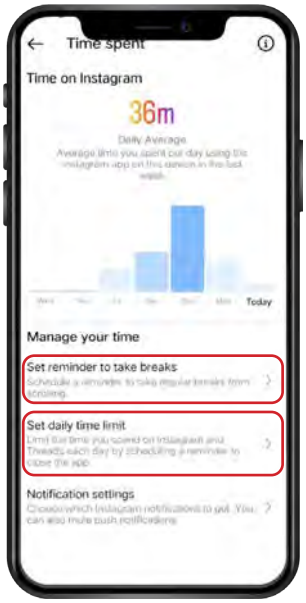
¿Cómo podemos configurar un Recordatorio de Tiempo?

1. Entra en 'Configuración' haciendo clic en el ícono de tres líneas, en la parte superior de tu perfil.
2. Selecciona 'Tu actividad', y haz clic en 'Tiempo dedicado'.
3. Establece un límite de tiempo y haz clic en 'Programar recordatorio'.



¿Cómo acceder a los datos de Actividad?

1. Entra en 'Configuración' haciendo clic en el ícono de tres líneas, en la parte superior de tu perfil.
2. Selecciona 'Seguridad'y haz clic en 'Acceder a datos'.



TIK TOK

TikTok permite configurar funciones de bienestar digital, estas mejoran la protección del usuario/a y permiten aprender a usar la aplicación de forma responsable.

¿Qué te permite hacer la App?

- **Modo restringido:**
  Puedes configurar este filtro para impedir que se sugieran vídeos inadecuados para las NNA como madre, padre o cuidador debes tener en cuenta que este tipo de filtros pueden permitir el acceso a algunos vídeos que se consideren inapropiados para determinadas edades, por lo que requieren acompañamiento y supervisión.

- **Límite de tiempo:**
  Permite configurar un periodo de tiempo diario para usar la aplicación.

- **Filtrado de contenidos:**
  Es posible establecer la cuenta como privada, restringir los comentarios o configurar un filtro que bloqueará aquellos que se consideren ofensivos o que contengan una palabra determinada.

¿Cómo configurar un Recordatorio de Tiempo?

1. Entra en 'Configuración' haciendo clic en el icono de 3 puntos, en la parte superior de tu perfil.
2. Dentro del menú, ve al apartado 'Privacidad y ajustes' y selecciona 'Desintoxicación digital'.
3. A continuación, haz clic en 'Gestión de tiempo en pantalla' y escoge el tiempo que consideres adecuado, pulsa el botón para activar y crea un código.
4. Una vez terminado el tiempo establecido para cada día, tu hija o hijo deberá introducir el código para poder continuar usando la aplicación.

¿Cómo pasar una cuenta de pública a privada?

1. Entra en 'Configuración' haciendo clic en el icono de tres puntos situado en la parte superior de tu perfil.
2. Dentro del menú ve al apartado 'Cuenta', selecciona la opción 'Privacidad y seguridad', enseguida activa la opción 'Cuenta privada' y desactiva la opción 'Recomienda tu cuenta a otros'.

YOUTUBE

YouTube ofrece funciones de control parental, que se pueden configurar dentro de los ajustes de la cuenta,

¿Qué te permite hacer la App?

- **Modo restringido o seguro:**
  Permite descartar en las búsquedas contenidos calificados para adultos, impidiendo a su vez acceder a los comentarios de todos los vídeos que se reproduzcan. Se activa a nivel de navegador o aplicación, no en la configuración de la cuenta. Por lo tanto, es necesario activarlo en cada aplicación o dispositivo de forma manual, y tener en mente que es un ajuste que cualquier usuario puede modificar sin autorización.

- **Sincronización con Family Link:**
  Ofrece la opción de activar el modo restringido de la aplicación desde el dispositivo que actúa como administrador, impidiendo que la NNA pueda desactivar las opciones de control establecidas.

¿Cómo activar el modo restringido o seguro en un dispositivo Android?

1. Entra en los ajustes de tu cuenta, haciendo clic en los tres puntos de la parte superior derecha.
2. Haz clic en 'Ajustes' y luego selecciona 'General'.
3. Activa el 'Modo restringido'.

¿Cómo activar el modo restringido o seguro en un dispositivo iOS?

1. Entra en los ajustes de tu cuenta, haciendo clic en tu imagen de tu perfil.
2. Selecciona 'Ajustes'.
3. Activa el 'Modo restringido'.

UBER, INDRIVER o alguna otra app de transporte

Usar apps de transporte se ha convertido en un hábito cotidiano. Sin embargo, al usar estas aplicaciones también podemos encontrar riesgos, por lo que te presentamos algunas recomendaciones de seguridad dentro y fuera de la aplicación.

Consejos de seguridad para proteger tus datos en la app

- Nunca compartas tu contraseña de acceso a la app.
- Si recibes un mensaje aparentemente de la app, verifica que provenga de cuentas oficiales.
- Usa la verificación en dos pasos.
- La única forma de solicitar un servicio, u obtener una cuenta, es a través de las aplicaciones, no caigas en engaños con servicios ofrecidos por otras vías, como son las redes sociales.
- Al usar uber, implementa el código de verificación de 4 dígitos recibido por SMS.
- No compartas ni divulgues tu código Uber de verificación de 4 dígitos recibido por SMS, este número es para tu uso exclusivo y ningún agente de soporte lo solicitará.

¿Cómo implemento la Verificación de viaje con PIN en uber?

Usar el código de verificación para iniciar un viaje, te permitirá estar seguro de que estas abordando el vehículo oficial que te asignó la aplicación y evitar riesgos.

1. Entra a la aplicación y dirígete al **apartado de cuenta ubicado en la esquina inferior derecha.**
2. En la opción de **"Configuración" (Settings) seleccionar "Verificar viajes" en el apartado de seguridad.**
3. Elegir entre **activar la función código PIN para todos los viajes o solo en aquellos que se hagan en un horario determinado.**

Consejos de seguridad para proteger durante el viaje

- Pide un viaje sin salir de donde estés, minimiza el tiempo que permaneces en solitario afuera con el teléfono en la mano.
- Verifica los datos del viaje, cada vez que viajes, verifica la matrícula, la marca, el modelo del auto y la foto del conductor que aparecen en la app para asegurarte de subir al auto correcto.
- Pídele al conductor que confirme tu nombre, además de seguir los pasos para verificar los datos del viaje, puedes pedirle al conductor que confirme tu nombre antes de subirte al auto.
- Comparte los detalles del viaje con tus seres queridos.
- Viaja en el asiento trasero siempre que sea posible, en especial si viajas solo, esto te permite usar cualquiera de las puertas para evitar el tránsito al descender del vehículo y les da un poco de espacio personal tanto a ti como al conductor.

Control parental en Consolas de Videojuegos

Videojuegos y sus categorías

¿Para qué me sirve conocer las categorías?

Conocer las edades a las que van dirigidos los títulos de videojuegos que se encuentran en el mercado, será de gran utilidad para identificar a que contenido están expuestos tus hijos o hijas.

Clasificación "A"
Contenido para todo público

El contenido es apto para todas las edades, puede que contenga una cantidad mínima de violencia de caricatura, de fantasía o ligera, o uso poco frecuente de lenguaje soez moderado.

Clasificación "B"
Contenido para adolescentes a partir de 12 años

Puede que contenga más violencia de caricatura, de fantasía o ligera, lenguaje soez moderado o temas insinuantes mínimamente provocativos.

Clasificación "B15"
Contenido para mayores de 15 años

Pueden contener violencia, temas insinuantes, humor vulgar, mínima cantidad de sangre, apuestas simuladas o uso poco frecuente de lenguaje fuerte.

Clasificación "C"
Contenido no apto para menores de 18 años

Pueden contener violencia intensa, derramamiento de sangre, contenido sexual o lenguaje fuerte.

Clasificación "D"
Contenido extremo y exclusivo para adultos

Pueden incluir escenas prolongadas de violencia intensa, contenido sexual gráfico o apuestas con moneda real.

Las especificaciones de contenido sirven como guía del contenido que pudiera aparecer en los videojuegos asignados a cada categoría.

Puedes encontrar esta estampa con la clasificación ubicada de manera impresa o con una etiqueta adherida a la carátula frontal del producto.

Ahora que sabes como identificar el contenido de cada videojuego veamos como puedes protegerte cuando ya lo haz comprado.

CONTROL FAMILIAR MICROSOFT

Una vez creada la cuenta en Microsoft es posible establecer límites desde family.microsoft.com o desde la propia aplicación Microsoft Family Safety.

¿Qué te permite hacer la App?

Localización Familiar:

Es posible compartir la ubicación, guardar los lugares que el menor visite con frecuencia y activar las alertas de ubicación.

Filtrado de contenido:

Controlar las aplicaciones como los juegos a los que la NNA podrá acceder, se puede establecer una clasificación en función de rangos de edad y tipos de contenido, ademas de seleccionar los programas que podrá usar tu hija o hijo.

Límite de Tiempo:

Controlar el tiempo que las NNA podrán hacer uso del equipo.

Establecer límites de aplicaciones y juegos en family.microsoft.com

1. Inicia sesión con tu cuenta de Microsoft en **family.microsoft.com**
2. Busque el nombre de tu hija o hijo y seleccione **'Límites de aplicaciones y juegos'.**
3. Encuentre la **aplicación o juego para el que quiere establecer límites.**

¿Quieres conocer más sobre el Control familiar Microsoft?, podemos ayudarte, **escanea el QR o ingresa a https://www.microsoft.com/es-es/microsoft-365/family-safety**

CONTROL FAMILIAR XBOX

La consola Xbox One permite configurar ajustes de control parental, creando un grupo de cuentas familiar administrado por un adulto.

¿Qué nos permite hacer?

- **Seguimiento de actividad:**
  Puedes recibir un informe semanal por correo electrónico con un resumen de las sesiones de juego, la duración de las mismas, los juegos y contenidos a los que ha accedido la NNA y durante cuánto tiempo.
- **Notificaciones:**
  Te llegará un aviso para que aceptes o deniegues la solicitud de tu hija o hijo cuando quiera acceder a un contenido concreto o realizar una compra.
- **Filtrado de contenido:**
  Es posible limitar los juegos a los que puede acceder la NNA, las búsquedas web y páginas concretas.
- **Límite de Tiempo:**
  Permite configurar un recordatorio diario de tiempo, que avisará al menor cuando haya superado el tiempo establecido.
- **Permitir y bloquear programas específicos:**
  Es posible restringir el acceso a aplicaciones y juegos determinados por el administrador familiar, así como limitar las compras en la tienda virtual.

¿Cómo configuramos un limite de tiempo?

1. **Accede al menú** de tu cuenta desde la consola o desde el ordenador.
2. **Inicia sesión** con tu cuenta de usuaria/o.
3. **Puedes configurar el límite de tiempo** para uno o varios dispositivos.
4. **Establece el horario** o el período de tiempo que consideres adecuado.

¿Quieres conocer más sobre el Control familiar EN XBOX?, podemos ayudarte, **escanea el QR o ingresa a https://www.xbox.com/es-ES/community/for-everyone/responsible-gaming**

CONTROL FAMILIAR NINTENDO SWITCH

La consola Nintendo Switch ofrece opciones de control parental en la consola y por medio de una app.

¿Qué nos permite hacer?

- **Límite de Tiempo:**
  Puedes configurar un horario semanal de tiempo de juego permitido, cuando la sesión de juego se acerca al tiempo establecido, una alarma avisa a tu hija o hijo para que apague la consola, también es posible activar la función 'suspender programa', para que la consola salga del juego de forma automática al terminar el tiempo.

- **Filtrado de contenido:**
  Permite restringir aquellos juegos que no son apropiados para tu hija o hijo, según la clasificación de edades establecida, además, es posible impedir la comunicación con otros usuarios y la publicación de capturas de pantalla en las redes sociales.

- **Control multidispositivo:**
  La aplicación permite supervisar la actividad de varios usuarios desde el dispositivo que actúe como administrador.

Además, es posible configurar algunos ajustes en la propia consola sin necesidad de descargar la aplicación, como el filtro de contenidos por edades.

¿Cómo configurar la aplicación Control parental de Nintendo Switch?

1. **Descarga la aplicación** en tu móvil desde Google Play, App Store o desde el enlace de la página oficial de Nintendo.
2. Una vez instalada, **inicia sesión en tu cuenta Nintendo, o crea una nueva** siguiendo los pasos que se indican en la aplicación. Después, **aparecerá un código de verificación que debes introducir en la consola para vincularla.**
3. Para ello, enciende la consola Nintendo Switch, entra en las **opciones de configuración de la consola y haz clic en 'Control parental'.**
4. Entra en 'Ajustes de control parental' e **introduce el código de verificación,** Ahora puedes establecer las restricciones y límites que consideres adecuados desde tú móvil.

¿Quieres conocer más sobre el Control familiar en Nintendo Switch?, podemos ayudarte: **https://www.nintendo.es/Atencion-al-cliente/Nintendo-Switch/Como-iniciar-sesion-en-una-cuenta-Nintendo-1378976.html**

CONTROL FAMILIAR PLAYSTATION

La consola PlayStation ofrece algunas funciones de control parental para aumentar la protección de los menores.

¿Qué nos permite hacer?

- **Límite de Tiempo:**
  Filtrado de contenido:
  Es posible establecer una restricción de edad para los juegos y otros contenidos audiovisuales, al conectarse a Internet en Playstation Network, es posible impedir la comunicación con otros usuarios de Playstation y el acceso a contenidos creados por otros jugadores.

- **Bloqueo de aplicaciones:**
  Permite restringir las compras en la tienda virtual de Playstation creando un límite de gasto mensual.

- **Límite de Tiempo:**
  Puedes establecer un horario semanal de tiempo de juego, una duración para cada sesión de juego y/o una hora de finalización.

¿Cómo establecer un control de tiempo en PlayStation 4 y 5?

1. Desde tu consola Playstation, **accede a 'Ajustes'.**
2. Selecciona **'Control Paterno',** y después '**Administración de familia'.**
3. **Introduce la contraseña** de tu cuenta de usuario/a.
4. **Selecciona el usuario/a** que quieres restringir.
5. **Configura una 'Zona horaria'** y luego selecciona **'Ajustes para tiempo de juego'.**
6. **Establece los límites de tiempo** y haz clic en 'guardar'.

Además, es posible especificar una contraseña de seguridad, de tal forma que el menor no pueda modificarlos, ni tampoco crear nuevas cuentas de usuario.

¿Quieres conocer más sobre el Control familiar EN Playstation?, podemos ayudarte: **https://www.playstation.com/es-mx/support/account/ps4-parental-controls-and-spending-limits/html**

Instituciones amigas

¿Dónde puedes pedir ayuda?

¿Tienes dudas o no sabes cómo actuar ante alguna problemática?, conoce las instituciones que pueden darte asesoría y apoyo ante alguna problemática, tu familia siempre puede estar cibersegura con el apoyo de tus instituciones amigas.

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

La jefatura cuenta con personal capacitado que pueden apoyarte y guiarte si piensas que eres víctima de algún delito informático, o si solo buscar información adicional para mantener seguras las cuentas de tu familia, podrán brindarte información y posibles soluciones a la problemática que te enfrentas, además de contar con diferentes canales de comunicación en caso de que no puedas ir personalmente, pero requieras información, ¡Comunícate!

¿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 X (antes 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

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

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