

## INFORME TALLER 2 A 40 DOCENTES SOBRE EIS

|   |  |
|---|--|
| <b>Reportado por:</b> <b>Gandhy Velásquez</b>   | <b>Fecha del reporte:</b> <b>10/08/2020</b>            |
| <b>Resultado:</b> <b>2.3.1</b>  |  |
| <b>Nombre de la actividad:</b> <b>Autoridades</b>   |  |
| <b>Nombre de la subactividad:</b> <b>'El uso de la tecnología y las redes sociales como herramientas de riesgos para la niñez, adolescencia y juventud'</b>   |  |
| <b>Hora inicio:</b> <b>9:00</b><br><b>Hora finalización:</b> <b>11:00 am</b>  | <b>Participantes:</b> 40<br>Hombres: 23<br>Mujeres: 17 |
| <b>Lugar:</b> <b>Forma virtual, Huehuetenango</b>   | <b>Fecha:</b> <b>10 de agosto</b>                      |
| <b>Objetivos:</b> <ol style="list-style-type: none"> <li>1. Informar a los docentes sobre el uso de las nuevas tecnologías de la información y comunicación como herramienta de riesgo y vulneración de los derechos de la niñez, adolescencia y juventud</li> <li>2. Establecer acciones estratégicas en los establecimientos educativos, con la finalidad de identificar los posibles riesgos derivados del uso de la tecnología de la Información utilizada por el estudiantado</li> <li>3. Enlistar a las entidades, públicas o privadas del ámbito de las nuevas tecnologías, que faciliten información sobre las ventajas y desventajas del uso.</li> </ol>   |  |
| <b>Descripción de la Actividad:</b>   |  |
| <b>Puntos de agenda:</b> <ol style="list-style-type: none"> <li><b>1. Normas de convivencia de la reunión virtual</b><br/>Al ingreso a la plataforma se socializaron las normas mínimas: Micrófono en silencio, levantar la mano para participar, intervenciones puntuales, entre otras indicaciones. Con la finalidad de cumplir con los tiempos y se mantuviese el orden en las intervenciones en cada punto de agenda.</li> <li><b>2. Bienvenida y presentación de objetivos del taller y presentación de facilitador del taller</b><br/>Estuvo a cargo del equipo facilitador de OSAR Juvenil Huehuetenango, quien habilitaron su cámara para que el grupo participante las/os visualizaran al momento de dar a conocer la bienvenida y socialización de los objetivos del taller, así como la presentación del facilitador y de esta manera dar por inaugurado el taller e iniciar a desarrollar la presentación de cada tema.</li> <li><b>3. Conocimientos previos.</b><br/>Al iniciar la presentación introductoria del tema, se socializaron las 3 preguntas generadoras a las y los participantes, tomando en cuenta que con tiempo de antelación les fueron compartidos algunos documentos sobre los temas a abordar.<br/><br/>Conocimientos previos: ¿Qué ventajas tiene el uso del internet y las redes sociales? - ¿Qué desventajas tiene el uso del internet y las redes sociales? - ¿Qué es un delito cibernético? - ¿Conocen alguna experiencia sobre el delito cibernético? Realimentación de aprendizajes.</li> </ol> |  |

Por razones de tiempo, se solicitó que agregaran sus respuestas en el chat de la reunión, para que durante las intervenciones se puedan retomar aspectos importantes para ser ampliados, permitiendo la participación de 2 adolescentes y jóvenes para que enciendan su micrófono y compartieran sus puntos de vista y respuesta a una de las interrogantes por persona.

#### **4. Abordaje del fenómeno del ciberdelito en el aula Socialización de videos Realimentación de aprendizajes.**

Socialización del manual del curso de prevención del ciberdelito para profesores creado por UNODC y SVET.

Es la práctica para defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de las tecnologías de la información o seguridad de la información electrónica.

El término es más amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres.

- **Riesgo:** Es la probabilidad de que se produzca un incidente al materializarse una amenaza que explote la vulnerabilidad y que cause pérdidas o daños.
- **Amenaza:** Es toda acción que aprovecha una vulnerabilidad para atentar contra el sistema completo, sus componentes o actividades.
- **Vulnerabilidad:** Es una debilidad o fallo en un sistema que pone en riesgo a sus componentes o actividades.
- **Daño:** es la afectación real y efectiva en el sistema, sus componentes o actividades.

#### Factores que estimulan el riesgo del Internet:

- Anonimato (casi completo).
- Suplantación o robo de identidad.
- Impostura, simulación de una identidad/vida distinta.
- Ausencia de datos "de contexto" en las relaciones.
- Alta disponibilidad (24/7).
- Máxima rapidez de propagación.
- Bajo coste (conexión, replicación).
- Dificultad de seguimiento por parte de la justicia.
- Reducción de distancias.
- Facilidad de geolocalización y confluencia.
- Características adecuadas para contenidos audiovisuales.
- Nuevas formas de delito y abuso.
- Dificultad y/o desinterés en verificar la edad del usuario.
- Consolidación como espacio de socialización.
- Tendencias: Reducción de la edad de inicio en el uso de la Red.
- Mayor ancho de banda y uso de contenidos audiovisuales.
- Accesibilidad e inmediatez (móviles).
- Web 2.0... protagonismo del usuario como editor y auge de las redes sociales.

#### A través de internet hay un **aumento** de:

- Cyberbullying.
- Grooming y ciber violencia de género.
- Amenazas a la privacidad.
- Imágenes de abuso sexual infantil.

- Delitos cometidos por menores.
- Uso abusivo y juegos de azar/apuestas.

#### Conexiones no seguras:

- Alguien interfiere en tu conexión a la red y entra a través de la red en tus dispositivos (en casa, en otros sitios).
- La conexión va muy lenta en casa (podría haber usuarios desconocidos conectados a nuestro router utilizando nuestro 'ancho de banda')
- Conectado a redes wifi no seguras (centros comerciales).
- Conectado a redes wifi 'gratuitas' o abiertas fraudulentas. Muchos adolescentes, para ahorrar datos, instalan software para buscar wifis abiertas o 'fáciles de crackear y pensando que están 'robando' wifi pueden estar cayendo en la trampa de alguien.

#### Enlaces Fraudulentos:

- Llegan por comunicación directa (e-mail, WhatsApp, foros, redes etc... en cadenas, robots dedicados, spam...) o indirecta (banners anuncios,...) y redirigen, por lo general, a páginas web muy similares a las reales en las que el usuario debe rellenar un formulario.
- Algunos apelan a la caridad (imposibilidad de cobrar una herencia por estar en un país remoto), a la curiosidad ('entérate quién te ha borrado de su círculo de amigos'), a la "ingenuidad" (has sido el ganador de un coche) o a la amenaza (confirmación de datos indispensable por actualizaciones en el sistema).
- Si el usuario cumplimenta el formulario proporcionando los datos solicitados, estos datos acabarán almacenados en servidores controlados por ciberdelincuentes.

#### La prevención en Internet:

- Las políticas preventivas son parte sustancial del combate contra el crimen. Por esto es necesario dar impulso a programas y acciones integrales a nivel nacional, regional, estatal y municipal, con el fin de evitar que haya más personas que se conviertan en delincuentes, o que sufran violaciones a su integridad, patrimonio o que queden atrapados por el consumo de drogas. La función de la prevención social consiste en eliminar los problemas sociales que puedan llevar a un joven a delinquir o ser víctima de un delito.
- Como usuario de la red se pueden tomar varias medidas preventivas como mantener activados y actualizados los antivirus en nuestros dispositivos con conexión a internet, evitar realizar operaciones financieras en redes abiertas o computadores públicos y verificar los archivos adjuntos de mensajes de desconocidos y evitar descargarlos si no se tiene plena seguridad de su contenido.

#### Estrategias de Prevención:

- Uso de estrategias de comunicación educativa.
- Transversalidad con otros aspectos educativos (equidad de género, inclusión...).
- Promoción de valores universales (solidaridad respeto, cooperación...).
- Aplicación de metodologías innovadoras: procesos, medios, canales, agentes...
- Desarrollo de habilidades para la vida (pensamiento crítico, trabajo en equipo, empatía, y resolución de conflictos).

#### Decálogo de los derechos de las niñas y niños vinculados a su seguridad:

- **Derecho al acceso a la información** sin discriminación por sexo, edad, recursos económicos, nacionalidad, etnia o lugar de residencia. Este derecho se aplicará en especial a los niños y niñas discapacitados.
- **Derecho a la libre expresión y asociación.** A buscar, recibir y difundir informaciones e ideas de todo tipo por medio de la red. Estos derechos solo se restringirán para garantizar la protección de los niños y

niñas frente a informaciones perjudiciales para su bienestar, desarrollo e integridad; y para garantizar el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.

- **Derecho de los niños y niñas a ser consultados y a dar su opinión** cuando se apliquen leyes o normas a Internet que les afecten.
- **Derecho a la protección** contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo.
- **Derecho al desarrollo personal y a la educación**, y a todas las oportunidades que las nuevas tecnologías puedan aportar para mejorar su formación de manera **responsable**.
- **Derecho a la intimidad de las comunicaciones** por medios electrónicos. Este Derecho garantiza el no proporcionar datos personales por Internet, a preservar su identidad y su imagen de posibles usos ilícitos.
- **Derecho al esparcimiento, al ocio, a la diversión y al juego**, mediante Internet y otras tecnologías. Derecho a que los juegos y las propuestas de ocio no contengan violencia gratuita, ni mensajes racistas, sexistas o denigrantes y que respeten los derechos y la imagen de los niños y niñas y otras personas.
- Los padres y madres tendrán el **derecho y la responsabilidad de orientar y acordar con sus hijos e hijas un uso responsable**.
- Los gobiernos de los países desarrollados deben comprometerse a **cooperar con otros países** para facilitar el acceso de estos y sus ciudadanos, y en especial de los niños y niñas, a Internet y otras tecnologías para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los países pobres.
- **Derecho a beneficiarse y a utilizar en su favor las nuevas tecnologías** para avanzar hacia un mundo más saludable, pacífico, solidario, justo y respetuoso con el medioambiente, en el que se respeten los derechos de todos los niños y niñas.

**Definición bullying:** "Una conducta antisocial persecutoria y de agresión física, psicológica o moral que realiza un alumno o grupo de alumnos sobre otro, con desequilibrio de poder y de manera reiterada"

**Ciberacoso entre iguales ¿qué es?:** Es la situación de maltrato y hostigamiento reiterado, prolongado en el tiempo e intencionado hacia una persona por parte de otra u otras de similar edad usando las nuevas tecnologías digitales de la información y comunicación ligadas a Internet. Se alude de forma expresa con el término ciberbullying para situarlo en el entorno escolar por similitud con el bullying tradicional, pero también se produce con frecuencia fuera del mismo, incluso con la participación de personas desconocidas. Si se trata de personas adultas o de edades muy diferentes se debiera calificar como ciberacoso. Cuando hay intencionalidad sexual tampoco se debe aplicar el término ciberbullying. Tampoco debe ser confundido con el "linchamiento digital".

**Ciberbullying:** Es el uso de los dispositivos electrónicos a través del Internet, telefonía celular y videojuegos on-line para ejercer el acoso entre iguales en un mismo colegio, escuela, zona, región o país. El término ciberbullying se usa para situarlo en el entorno escolar por similitud con el bullying tradicional, pero también se produce con frecuencia fuera del mismo, incluso con la participación de personas desconocidas. Es el hostigamiento o acoso con burlas, insultos, amenazas y chantaje de un niño hacia otro de similar o igual edad, aunque también puede ser realizado por una persona adulta. Este maltrato verbal y psicológico provoca dolor, tristeza, angustia y desesperación en la víctima, por que este se da de manera reiterada.

**¿Cómo se manifiesta? :** Flaming: Luchas online a través mensajes electrónicos con lenguaje enfadado y soez.

- Denuncias injustificadas a los gestores de servicios online.
- Acecho y persecución con mensajes ofensivos e insultantes.
- Robo de contraseñas, impidiendo el uso o suplantando.
- Acoso con matices sexuales pero sin ese fin.
- Intimidación mediante amenazas.

- Denigración, creación de páginas o poner en circulación informaciones y bulos que dañen su reputación
- Revelación de información sensible o privada
- Exclusión deliberada de actividades online, integrando una "lista negra".
- Juego sucio e invalidante en el contexto de entornos lúdicos online.

### Ciberbullying vs Bullying: ¿Qué peligros añadidos presenta el ciberbullying?

- ✓ Puede ser más **oculto**, menos perceptible.
- ✓ El umbral de **relación inicial** preciso entre las partes es menor.
- ✓ Los abusadores pueden pedir ayuda incluso a **gente desconocida**.
- ✓ No hay modo de **escape a la presión**. Las comunicaciones online pueden crear mucha afición o dependencia y, en todo caso, son una parte de la vida del adolescente y transversal a sus otros contextos.
- ✓ El material lesivo se puede distribuir a todo el **mundo** y a veces es **irrecuperable**.
- ✓ Una acción concreta puede perdurar indefinidamente.
- ✓ El **liderazgo** en el grupo de acosador es menos manifiesto, más distribuido.
- ✓ No hay **patrones** claros predefinidos sobre potenciales víctimas y agresores e incluso estos roles son inversos en quienes están implicados en bullying.
- ✓ Las víctimas a veces optan por no pedir ayuda porque piensan que sus actividades online pueden ser consideradas la causa del problema y, en consecuencia, serles retirado **el acceso a la tecnología** (internet o móvil).
- ✓ Mayor desconocimiento sobre las **responsabilidades** derivadas de acciones.
- ✓ Menor **percepción del daño** causado.

### Decálogo para una víctima de ciberbullying estrategias de prevención

- ✓ Pide ayuda.
- ✓ No respondas a las provocaciones ni al chantaje.
- ✓ Trata de evitar aquellos lugares, o páginas donde eres hostigado.
- ✓ Cuida con celo tu privacidad en internet para disminuir ataque de acosadores.
- ✓ Guarda las pruebas del acoso en captura de pantalla.
- ✓ Asegúrate de decir a quien te acosa que te molesta lo que hacen.
- ✓ Hazles saber que lo que hacen como acosadores es perseguible por la Ley.
- ✓ Deja constancia de que estás en disposición de denunciar.
- ✓ Toma medidas legales.

### ¿Qué es el grooming?

**Grooming:** El grooming es una estrategia de ciberacecho sexual por parte de una persona adulta hacia una menor de edad. El depredador sexual, tras ganarse la confianza de la víctima mediante empatía, atención o adulación busca luego, generalmente con amenazas y chantajes, obtener concesiones de índole sexual (imágenes, vídeos o hasta un encuentro personal). La persona que hace grooming suele utilizar redes sociales, chats, juegos en línea o foros para contactar y hacer amistad con sus víctimas. Capta su interés con un perfil atractivo que le brinda confianza, expresa en sus conversaciones los mismos gustos y emociones y utiliza las mismas expresiones, lenguaje y emoticonos para ganar la simpatía con sus víctimas. Se presenta como el amigo, amiga, novio o novia ideal.

### Estrategias de Grooming ¿en qué consiste?

- ✓ Es la estrategia de acercamiento desarrollada por adultos pedófilos para ganarse la confianza del niño, niña o adolescente con el fin último de obtener algún tipo de gratificación de tipo sexual (imágenes, vídeos, encuentros...)
- ✓ Dibujan una estrategia de empatía y acercamiento tras estudiar a su presa.



- ✓ En ocasiones se hacen pasar por alguien de edad similar.
- ✓ Usan imágenes de tipo sexual para incitar, comprometer o normalizar.
- ✓ Una vez que consiguen alguna imagen "comprometida", la usan para el chantaje.
- ✓ Cuando tienen sus datos, pueden pasar a amenazar con hacer daño a la víctima y/o su familia.
- ✓ Ofrecen dinero para posar con poca ropa o desnudos frente a la cámara web.
- ✓ Prometen que los harán modelos.
- ✓ Puede haber manipulación de fotografías para después chantajear, y obligar a seguir abasteciendo de imágenes.

#### Otros riesgos del grooming: la trata de personas:

Es la captación, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación sexual, laboral, mendicidad o servidumbre y tráfico de órganos

- ✓ Pedófilo: Es la inclinación sexual por parte de adultos a sentir una atracción sexual primaria hacia niños o adolescentes.
- ✓ Pederasta: Es la práctica sexual entre un adulto y un menor de edad.

#### Perfiles de las víctimas y factores de riesgo

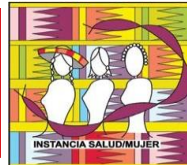
- ✓ Son en su práctica totalidad niñas adolescentes, pero también hay chicos que lo sufren y en todo caso la edad puede estar disminuyendo.
- ✓ La escasa percepción del riesgo o su inexperiencia son factores presentes con frecuencia (y por otro lado naturales en niñas, niños y adolescentes), pero no condiciones necesarias para que se dé un caso de grooming. Un descuido, la inmediatez de Internet o la extraordinaria habilidad del depredador juegan un gran papel que hacen de cualquier niña, niño o adolescentes una víctima potencia.
- ✓ Buscan presas más vulnerables: baja autoestima, escasa supervisión parental, muchas horas conectados, mala relación con sus padres o problemas familiares.
- ✓ La posibilidad de enviar o mostrar imágenes, como es vía webcam o Smartphone, sí es un factor crítico.
- ✓ En ocasiones, los factores de exclusión como escasos recursos económicos, bajo nivel cultural, discapacidad física o menor capacidad intelectual o pertenencia a un grupo social minoritario o discriminado son un factor determinante.
- ✓ En algunos casos, las prácticas de riesgo (estar con edad inadecuada en aplicaciones de contactos o similares) pueden ser un factor que facilite la acción del depredador.

#### 5. Conversatorio virtual: Como tratar de identificar a la víctima y cuál es el marco legal y sobre qué consejos dar a niños, niñas, adolescentes y adultos para el buen uso de la tecnología

En este espacio se logró analizar algunos de los casos que se viven como población vulnerable al momento de tener acceso a redes sociales sin una adecuada supervisión, máxime en menores de edad y como eso afecta no solo en la reputación de las personas cuando son víctimas de personas malintencionadas en internet, pero la preocupación al momento de que se han registrado casos de muertes como consecuencia de no tener precaución al momento de tener contacto con personas desconocida.

Y se trabajara en la creación de estrategias que permitan hacer evidente la importancia de abordar estos temas en todos los sectores de la población, ya que ante la nueva normalidad, lo virtual es algo que va en aumento.

| Resultado: | Recomendaciones: | Acciones de seguimiento: |
|------------|------------------|--------------------------|
|------------|------------------|--------------------------|



|  |  |   |
|--|--|---|
| <p>Análisis sobre situación actual de los delitos cibernéticos y como poder prevenir ser víctima.</p> <p>Se mejoró la participación de las y los adolescentes mediante la plataforma virtual, así como el interés de abordar estas temáticas.</p> <p>Se contó con la participación del total de participantes inscritos.</p> |  | <p><b>Acuerdos y compromisos:</b></p> <ul style="list-style-type: none"><li>Se enviara la presentación a quienes participan dentro del taller al grupo de WhatsApp</li><li>Se socializara el contenido abordado para poder dar seguimiento al proceso y de esta manera fortalecer las acciones en favor de las poblaciones vulnerables a estos delitos.</li></ul> |
| <p><b>Nombre y firma del director del proyecto:</b></p>  |  |   |