CIBERSEGURIDAD

Prevención de ciberbullying y fomento de una cultura digital propositiva para los adolescentes

Contenido teórico

Actualizado por Jesica Arizpe Rosales (2020)
Realizado por María José Silias Martínez (2017)

ÍNDICE

Antecedentes

El tema del bullying o el acoso escolar es un tema aparentemente reciente que ha llamado la atención de maestros, padres de familia y sobre todo de los principales afectados que son los niños, adolescentes y jóvenes. El estudio sobre el acoso escolar encuentra sus precedentes varios años atrás con la colaboración de Dan Olweus, catedrático de Noruega, quien es el pionero en el tema al trasladar sus investigaciones de acoso laboral al ámbito educativo en 1973. Por lo tanto hay ya un total de más de cuatro décadas donde ha evolucionado tanto la investigación, como la prevención en estos temas; sin embargo, lo han hecho también las modalidades en el maltrato, la agresión y el acoso, una de ellas es el "ciberacoso" y una de sus modalidades, el "ciberbullying".

Gran importancia del crecimiento del ciberbullying está directamente relacionado con la cantidad de usuarios con servicio de internet, de acuerdo a los reportes del ENDUTIH, con resultados del 2018, el 52.9% de los hogares (18.3 millones) contaban con una conexión a internet, mientras que el año anterior era de un 50.9%. También se registraron 74.3 millones de usuarios en Internet de seis años o más, los cuales representan el 65.8% de la población total de ese rango de edad y un crecimiento de 4.2% respecto el año anterior.

El ciberespacio

Para poder hablar de ciberseguridad, es necesario mencionar el internet y el *ciberespacio,* puesto que éste es el contexto en que se desarrolla nuestro segundo término a desarrollar: el acoso escolar cibernético a prevenir.

Internet ha cambiado el modo en el que comprendemos las comunicaciones y, por lo tanto, el mundo, tanto a nivel doméstico en nuestras relaciones personales, como a nivel profesional y económico, la velocidad de la Red y las posibilidades que otorga han sido determinantes en los pocos años que llevamos de siglo XXI. Hoy en día es difícil encontrar

---

[1] "Métricas de Ciberseguridad en México" del SIU: The Social Intelligence Unit. Agosto 2, 2017.

[2] **Tecnologías de la Información y la Comunicación (TIC)**: Todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y vide

a alguien que no haya oído hablar de Internet, pero no todo el mundo tiene claro lo que es exactamente ni cómo nace, esta telaraña mundial a la que hoy se conecta medio planeta.

El nombre Internet viene de las palabras en inglés *Interconnected Networks*, que significa "redes interconectadas", de tal forma que Internet es la unión de todas las redes y computadoras distribuidas en el mundo, pudiéndose definir como una red global en la que se conjuntan todas las redes que utilizan protocolos específicos de TCP/IP (Transmission Control Protocol=Protocolo de Control de Transmisión, IP) y que son compatibles entre sí. En esta red de redes, participan computadoras de todo tipo, como grandes sistemas (instituciones oficiales, gubernamentales, educativas, científicas, empresariales, de ocio y demás) que pueden poner o no su información a disposición de los usuarios; así como también modelos personales.

Internet fue el resultado de un experimento del Departamento de Defensa de Estados Unidos en 1969, que se gestó por el desarrollo de "ARPAnet", una red que buscaba enlazar universidades y centros de alta tecnología para intercambiar datos entre científicos y militares. A la red se unieron *nodos* (punto de intersección) de Europa y del resto del mundo, formando lo que ahora se conoce como World Wide Web o "www" en español: la gran telaraña mundial, promoviendo que en 1990 ARPAnet dejara de existir.

De esta forma, el ciberespacio se refiere al espacio no físico creado por equipos de cómputo interconectados que permiten la interacción de sus usuarios, llamados *cibernautas,* en comunidades donde pueden interactuar en diferentes modelos económicos, sociales y educativos, entre otros, a través de Internet, para satisfacer sus necesidades a través de productos o servicios que se ofertan en esa comunidad.

Medios y usos

De esta forma, para acceder al ciberespacio sólo se necesita un dispositivo con acceso a internet, que serían las TIC's (Tecnologías de la Información y Comunicación)[2] y navegar en cualquiera de los medios que a continuación revisaremos brevemente:

[2] **Tecnologías de la Información y la Comunicación (TIC)**: Todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego. Recuperado de: http://tutorial.cch.unam.mx/bloque4/lasTIC el 25 de julio del 2017.

- Correo electrónico. Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos. Existen públicas (Gmail, Hotmail, etc.) y privadas (@nemi.com.mx por ejemplo).

- Redes sociales. Estructuras sociales compuestas de grupos de personas, conectadas por uno o varios tipos de relaciones, debido a que establecen lazos de familiaridad basados en la estructura de "conocido a conocido". Operan de acuerdo a las "3C": Comunicación, Comunidad, Cooperación. Pueden dividirse en las siguientes categorías:

    - Según finalidad.
        - De ocio. Aquellas que permiten la interacción entre usuarios sin ningún fin específico, más que compartir y contactarse (Facebook).
        - De uso profesional. Aquellas que tienen la intención de compartir un uso profesional (LinkedIn).
    - Según modo de funcionamiento.
        - De contenidos. Normalmente utilizados por marcas, donde generan "contenidos" *propios* o *curados*[3] para permanencia del cliente (Twitter de Comex: @PinturasComex).
        - Basada en perfiles: personales/profesionales. Son compatibles de acuerdo a la categoría de finalidad.

    - Según grado de apertura. De acuerdo a la capacidad de acceso a las mismas por cualquier usuario, tomando en cuenta un nivel o no de restricción:
        - Públicas. Abiertas a todo público (Facebook, Twitter, YouTube, Instagram)
        - Privadas. Abiertas únicamente a un grupo u organización específica, la cual se hace cargo del sistema (Slack para grupos específicos de trabajo).

[3] **Contenidos propios**: Contenidos que la marca genera. **Contenidos curados**: Aquellos no propios, pero que respetando la autoría de otra marca, comparten, pues va de acuerdo a su esencia de marca. Recuperado de la revista electrónica Forbes: https://www.forbes.com.mx/tipos-de-contenidos-en-redes-sociales-y-su-uso/ el 14 de julio de 20 17.

- Según nivel de integración. Toma en cuenta el nivel de afinidad e interés en integración de materias o actividades de tipo, preferentemente profesional.
    - Vertical. Basadas en un tema en concreto, buscan congregar a un gran número de usuarios afines (Flickr-fotografía, Vevo-música, YouTube-video).
    - Horizontal. Son transversales en cuanto a temáticas y se centran más en los contactos (Facebook-contactos, LinkedIn-profesional, Twitter-*microblogging*[4]).

- Banca en línea: Plataforma electrónica producida por cada institución bancaria que permite realizar pagos electrónicos de manera segura y cómoda de acuerdo a la CONDUCEF.

- Comercio electrónico. De acuerdo a la OCDE (Organización para la Cooperación y Desarrollo Económicos) es el proceso de compra, venta o intercambio de bienes o servicios e información a través de las redes de comunicación. Existe en México la Ley Federal de Protección del Consumidor en su capítulo VIII bis[5], que vela por la seguridad de los *ciberconsumidores*.

- Juegos en línea. Juegos digitales que requieren una conexión de red activa[6] para llevarse a cabo y permiten la creación de comunidades entre sus usuarios.

Ahora bien, ya que vimos todos los medios posibles de interacción, es importante mencionar también los "peligros" a los que se está expuesto, ya que como seres humanos no sólo tenemos un buen manejo de los medios informáticos, sino que desgraciadamente existen personas malintencionadas (más adelante revisaremos definiciones y causas) que buscan darle otro uso a estos medios que generalmente se crearon con intenciones de comunicación, comunidad o cooperación.

[4] **Microblogging**: Sistema que permite el envío y la publicación de mensajes breves, generalmente sólo de texto.
[5] Recuperado de https://www.profeco.gob.mx/internacionales/com_elec.asp el 14 de julio de 2017.
[6] Recuperado de http://www.pegionline.eu/es/index/id/53 el 14 de julio de 2017.

- Delito informático o ciberdelito contra niños (as) y adolescentes: Acciones antijurídicas que ocurren por vías o medios informáticos en contra de la integridad de niñas, niños y adolescentes.

- Conductas ilícitas informáticas:
    - Hackeo: Acción de entrar de forma abrupta y sin permiso a un sistema de cómputo o una red.

    - Spyware o keylogger: Software o hardware instalado en una computador, generalmente sin el conocimiento del usuario, que recoge información de dicho usuario para más tarde enviarla por internet a un servidor remoto y hacer uso de ella.

    - Scam: Intentos de estafa a través de correo electrónico o páginas web fraudulentas para obtener información o recursos económicos.

    - Bulo/hoax: Un bulo o noticia falsa es un intento de hacer creer a un grupo de personas que algo falso es real (el término *hoax* se popularizó al referirse a engaños masivos por medios electrónicos).

    - Phishing (suplantación de identidad): Abuso informático que se comete mediante el uso de un tipo de ingeniería social[7], caracterizado por intentar adquirir información confidencial de forma fraudulenta, por ejemplo contraseñas, información bancaria).

    - Sexting: Conducta de envío de contenidos eróticos o pornográficos por medio de teléfonos móviles o mensajes SMS.

    - Grooming: Hace referencia a una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando conexión emocional con éste, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.

[7] **Ingeniería social:** Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Recuperado de: https://www.seguridad.unam.mx/historico/documento/index.html-id=36 el 18 de julio de 2017.

- Pornografía infantil: Abuso y explotación sexual de menores de edad con algún fin de lucro.

- Prostitución infantil en internet: Acto de ofrecer en internet los servicios de un niño, niña o adolescente para realizar acciones sexuales a cambio de dinero, comida y/o techo.

- Turismo sexual en internet: Acto de ofrecer paquetes turísticos por internet en donde se ofrecen niñas, niños y adolescentes para sostener encuentros sexuales.

- Ciberacoso: Uso de medios de comunicación digitales para acosar a una persona o grupo de personas, mediante ataques personales, divulgación de información confidencial o falsa entre otros medios.

Conviene mencionar que, en temas de ciberseguridad, el Índice de Ciberseguridad Global de 2019, realizado por la Unión Internacional de Telecomunicaciones (UIT), reporta que México cayó 35 lugares con respecto a los resultados de 2017, ocupando la posición 63 de 175 países, con un índice de "0.629". [8]

Comprendiendo la problemática

Agresión y violencia

Durante el paso de los años, el ser humano se ha enfrentado a un sinfín de situaciones donde se pone en duda la "bondad y maldad" de su naturaleza: robos, traiciones, guerras, hackeos, phishing, agresiones y demás, sin embargo, aunque no nos entretendremos en el análisis de los actos humanos desde una perspectiva ética, sí nos enfocaremos en la descripción de los elementos que entran en el tema de nuestro interés: el ciberbullying y la ciberseguridad, para ello será necesario exponer los temas que se encuentran directa e indirectamente relacionados.

[8] "Métricas de Ciberseguridad en México" del SIU: The Social Intelligence Unit. Agosto 2, 2017.

Cuando hablamos de acoso, debemos entrar también a la definición de términos como violencia y agresión, los cuales aunque no son iguales, sí guardan una fuerte relación. Citando el marco teórico de nuestro tema de "Bullying" en NEMI, tenemos que en términos técnicos podríamos resumir la cuestión afirmando que la impulsividad es connatural al ser humano, no así la **violencia** que se manifiesta como una conducta aprendida por parte de éste, en el cual *la impulsividad se ordena a la consecución de un fin*.

La **agresión** es una *acción dirigida a dañar a otros*, y puede tener diversas modalidades como física, verbal, relacional o psicológica y que puede dividirse en dos tipos determinados: reactiva e instrumental. La **agresión reactiva** o también nombrada expresiva es aquella respuesta de corte impulsivo que un sujeto puede manifestar ante lo que él considera un ataque u ofensa por parte de otra persona, o bien se representa como una reacción a una frustración, casi siempre posterior a una provocación previa.

La **agresión instrumental** es aquella respuesta que busca igualmente dañar pero que no cuenta con justificación alguna por parte de quien ejecuta la conducta contra otra persona, sin embargo tiene la intención de alcanzar un fin o ganar cierta posición o estatus proveniente del cumplimiento de los objetivos propios del agresor, por lo tanto encaja con nuestro concepto de violencia.

Las diferencias entre ambos tipos de agresión varían entre las perspectivas utilizadas: social, emocional y cognitiva de acuerdo a la personalidad identificada de quienes la ejecutan. A continuación las podrás observar:

Diferencias	Agresión reactiva	Agresión instrumental (Violencia)
Perspectiva social	Quienes la ejecutan son rechazados, aislados y poseen un estatus social bajo en sus grupos de relación.	A pesar de no ser bien vistos, quienes la ejecutan pueden ser admirados y temidos por la mayoría. Pueden tener un alto nivel de popularidad en su grupo de relación e incluso se les llega a considerar líderes.
Perspectiva emocional	Está relacionada con dificultades para regular las propias emociones, especialmente el enojo	No tiene una relación clara con el manejo de emociones. Quienes la ejecutan pueden mostrarse muy calmados al momento de agredir, dan

	Intempestivo o la impulsividad.	la impresión de frialdad y de carencia de empatía frente al objetivo de las agresiones. No existe sentimiento de culpa en quien la ejerce.
Perspectiva cognitiva	Suele suponer que los otros siempre tienen la intención de hacerle daño (exista o no información que lo confirme). Por esto, aumenta la posibilidad de responder agresivamente ante cualquier acción de otros, ya que se actúa con una especie de paranoia constante.	Relacionada con la tendencia de considerarla un medio para obtener fines personales que interesan a quien la ejerce. Se recurrirá a ella una vez comprobada su efectividad, y se afirma con esto que es un comportamiento premeditado y calculado.

Es importante mencionar que en el ciclo de la violencia habrá siempre tres papeles definidos: **Agresor, víctima y testigos**, los cuales veremos más adelante.

Analizando estos datos, podemos llegar a diversas inferencias, como que la agresión que comúnmente utilizará un acosador en el contexto escolar será de corte instrumental, mientras que si la víctima responde a las agresiones con violencia, corresponderá a una agresión reactiva. De esta forma, el acoso escolar es también una agresión de tipo instrumental que responderá a los objetivos específicos del agresor.

Violencia escolar

María Victoria Trianes Torres, catedrática de la Universidad de Málaga, es una de las amplias referencias en cuanto a temas de violencia escolar se refiere. Propone que el acoso escolar o bullying es una de las manifestaciones de la violencia escolar, ya que ésta se refiere a toda clase de violencia que se suscite dentro del ambiente escolar y puede clasificarse de la siguiente manera: vertical y horizontal. La **violencia vertical** se ejecuta como un recurso de poder para ratificar la “autoridad” (o más bien un autoritarismo) con

la finalidad de mantener el control de los alumnos. Puede manifestarse de los maestros o administrativos hacia los alumnos.

La **violencia horizontal** en cambio, es aquella que se ejerce entre pares, es decir entre personas con el mismo rango de autoridad y similitud de condiciones, es decir los alumnos, pero con cierta diferencia de poder.

Trianes nos ofrece cuatro distinciones para tener mayor claridad respecto la violencia escolar:

Concepto	Definición
Conducta agresiva	Estrategia de resolución de conflictos interpersonales empleada para conseguir un objetivo personal (proactiva) y/o en respuesta a una agresión (reactiva).
Violencia interpersonal	Tipo particular de agresión dirigida hacia personas, se entiende que en el seno de relaciones sociales previamente establecidas.
Conducta agresiva antisocial	Comportamiento que no se ajusta a las normas y tiene graves consecuencias en el desarrollo del individuo, y en riesgo de quienes le rodean. Es un problema externalizante.
Violencia escolar	Agresiones de mayor o menor intensidad y gravedad que se dan en los contextos escolares, dirigidas hacia personas, propiedades y otras.

De esta forma, podemos entender que la violencia escolar es también un tipo de violencia interpersonal, ya que se da mediante la convivencia del contexto escolar. Por lo tanto el bullying es una manifestación más de la violencia presente en contextos escolares de corte horizontal, es decir se presenta en la relación interpersonal de los alumnos de un mismo salón o de una misma institución educativa; sin embargo, no excluye que la violencia escolar pueda presentarse sólo mediante el acoso escolar.

Posibles causas de la violencia escolar

Ya que hemos revisado la definición y las formas de manifestación de la violencia escolar, es necesario abordar sus posibles causas, que de acuerdo a Trianes se da en los cuatro principales ambientes de desarrollo de los agresores:

- **Familiar**. Esfera inherente a cada individuo en la que la institución educativa posee poca influencia, pero sí recibe repercusión en su organización escolar, debido a la influencia conjunta de los alumnos participantes o no en sucesos violentos. Se pueden destacar ciertas consideraciones de riesgo que pueden aumentar la probabilidad de la relación del alumno con sucesos violentos:
    - Falta de cariño, atención y comunicación por parte de los padres y/o tutores;
    - Separación, divorcio o ausencia de uno de los padres;
    - Ser hijo único con escasa red de amigos, primos, vecinos o pares con quienes convivir;
    - Falta de control y/o seguimiento de conductas por parte de padres y/o tutores;
    - Estilo de paternidad/maternidad autoritario, indefinido, democrático, etc.
    - Pobreza y falta de oportunidades.

- **Escolar**. Esfera referente a la organización interna del plantel y por la cual a pesar de las inconveniencias o riesgos provenientes de la familia, puede marcarse la pauta para la prevención y atención de problemáticas violentas. Se destaca lo siguiente:
    - Organización del plantel, claridad en funciones, responsabilidades y organigrama;
    - Presencia de un clima hostil dentro y en los alrededores del plantel;
    - Calidad en la relación profesor-alumno;
    - Carencia de normas y valores educativos en el proyecto de la institución (existencia y cumplimiento de un reglamento);
    - Indisciplina constante por falta de normas explícitas;
    - Ausentismo y retraso en los horarios de profesores o plantilla incompleta;
    - Racismo e intolerancia;
    - Fracaso escolar constante, alumnos repetidores.

- **Grupo de amigos**. Esfera que debe ser atendida en conjunto por la familia y la escuela, ya que los alumnos son influencia considerable para otros compañeros. Se destacan los siguientes patrones como causa de fenómenos violentos:
    - La existencia de pares que respaldan y aprueban el comportamiento violento como medio de obtención de diversos fines: estatus, reconocimiento, pertenencia y valorización de los miembros. De acuerdo a

Trianes, estos pares representan a los testigos activos (lo veremos más adelante).
    - Medio de generación de agresiones que aumentan en intensidad, inicia con transgresiones sencillas de las reglas que al no ser sancionadas invitan a una gradualidad en la gravedad de las conductas.

- **Medios de comunicación**. Esfera poco abordada por parte de padres y autoridades de planteles educativos, pero que supone una influencia de gran peso en la percepción que el alumnado integra respecto la violencia como mecanismo de resolución de conflictos. Se destacan como riesgo, los siguientes:
    - Violencia matizada y promovida desde ámbitos como música, videojuegos, películas, series, programas televisivos, noticias, publicidad y demás;
    - Acceso a mecanismos de tecnología para perpetuar y magnificar el impacto de la violencia.

Aunado a ello, es necesario comprender también la realidad respecto a los cambios que circundan la transición de nivel educativo a los que se enfrenta el adolescente, pues es también un cambio cultural:

- **Variación en el tamaño del plantel**. Generalmente, la escuela primaria es mucho más chica que una escuela secundaria; por lo tanto, el estudiante debe adaptarse al nuevo espacio físico.

- **Actividades estandarizadas**. A comparación del ritmo de clases de una escuela primaria, el nivel secundaria tiene mayor complejidad, pues existe la presencia de mayor cantidad de materias, entre ellas las de corte artístico y tecnológico, sin contar con la nueva complejidad que constituye el sistema de evaluación; por lo tanto le exige al alumno mayor atención y dedicación.

- **Varios profesores**. Por la especificidad de las materias, se designa un maestro por cada clase, que a comparación de la escuela primaria únicamente era uno, ahora son 8 los adultos con los que el adolescente debe establecer una relación y donde cada uno tendrá un estilo diferente de enseñanza; esto requiere del alumno un mayor ejercicio de sus capacidades de comunicación y de escucha activa.

- **Varias clases y varios compañeros**. La estabilidad e incluso comodidad que proporciona el tener un solo salón de clases se ve afectado cuando en la secundaria es necesario estar presente entre varios espacios físicos diferentes: salón, taller, laboratorio, biblioteca y demás, así como su convivencia con diferentes grupos de personas en los diferentes ambientes.

- **Diferenciación entre apto y no apto**. Aunado al nivel de evaluación mucho más complejo que la secundaria requiere, entra en juego la ratificación por parte de profesores, administrativos y otros profesionales involucrados, respecto aquellas personas que se presentan como más aptas que otras. El fracaso escolar y los alumnos repetidores tienen mayor reincidencia en el último año de la educación básica que en los años transcurridos en la primaria.

- **Amplitud de la localidad de origen**. Puesto que la cantidad de escuelas secundarias es menor a la de escuelas primarias, hay variación no solo en el tamaño de las instalaciones, sino también en la matrícula y las localidades de las que provienen los alumnos, por lo tanto varían también los estilos de vida de cada uno, creencias, tradiciones y maneras de configurar y comprender el entorno inmediato; por lo tanto existe una amplitud de interpretaciones, percepciones y significados no fáciles de asimilar, que al no encontrar adecuados mecanismos de diálogo y solución de conflictos, pueden llevar a la generación de distintos tipos de agresiones.

El alcance y la permanencia de la violencia escolar, expresada como bullying, no se relaciona únicamente con los involucrados y las afectaciones que éste les significa, sino que afecta también al propio proceso educativo del alumno complicándolo y obstaculizándolo, y en varias ocasiones inclusive anulándolo.

En cuanto fenómeno presente en la comunidad educativa, la violencia escolar tiene múltiples causas que son necesarias observar para prevenirlo de la forma más adecuada. No es un problema externo que no impacte al ámbito educativo, sino que proviniendo a veces de las esferas familiares, de grupo de amigos y de los medios de comunicación; pero siendo la comunidad educativa -destinataria y sustento de la vida del plantel- deber apoyar la resolución y erradicación adecuada de este conflicto.

Definiendo el fenómeno

Bullying

Ahora que ya sabemos lo que es y lo que no es la violencia escolar es importante pasar a la definición del bullying, ya que de éste depende nuestro siguiente tema a desarrollar.

El acoso escolar o bullying, como veíamos al inicio del documento, no es un tema nuevo en la sociedad, pero sí relativamente reciente en cuanto a su estudio, aunque el término se ha popularizado en los últimos años, gracias a campañas para poder contrarrestarlo por las graves consecuencias que se han observado en los alumnos, pero ¿qué es el bullying?

Olweus especifica que el acoso escolar se produce cuando un/os estudiante/s está/n expuesto/s, de forma repetida y durante un tiempo, a acciones negativas perpetradas por otros alumnos (1993), de tal forma que un estudiante está siendo intimidado cuando otro estudiante o grupo de estudiantes dice cosas mezquinas o desagradables, se ríe de él o ella o le llama por nombres molestos e hirientes. Le ignora completamente, le excluye de un grupo de amigos o le retira de actividades a propósito. Golpea, patea y empuja o amenaza. Cuenta mentiras o falsos rumores sobre él o ella. *El acoso escolar es la acción de molestar de forma repetida y de manera sumamente dañina y negativa*.[9] Asimismo es importante señalar que éste puede tomar la forma de cualquier tipo de violencia física, verbal, gestual, relacional e incluso sexual.

Mientras que Trianes complementa:

"Comportamiento prolongado de insulto, rechazo social, intimidación y/o agresividad física de unos alumnos contra otros que se convierten en víctimas de sus compañeros [...] se trata de relaciones de dominio-sumisión en las que se basan las prácticas cotidianas para controlar a otros, mediante la intimidación, la falta de respeto y la exclusión [...] Esta violencia es oculta y poco manifiesta a los ojos de los profesores, incluso soterrada, pero muy dañina para las víctimas, los agresores e incluso para los que son testigos o espectadores de los hechos".

Retomando a Olweus, podemos aterrizar tres características más sobre el acoso escolar:

[9] Santoyo Castillo, Dzoara; Frías, Sonia M. Acoso escolar en México: actores involucrados y sus características. Revista Latinoamericana de Estudios Educativos (México), Distrito Federal, 2014.

1. El acoso escolar es una **serie de conductas agresivas sin justificación** ejecutada por un alumno que **busca dañar** a otro;
2. Esta serie de conductas agresivas **se mantienen en el tiempo y no son episodios aislados**, sino que es posible describir cierta continuidad en los ataques que son repetitivos y que **aumentan con gradualidad**, junto con el peligro, promoviendo el daño.
3. Aunque la relación entre alumnos es horizontal, existe una relación de poder desequilibrada donde ellos: agresor y víctima, pasan a ser un fuerte y un débil.

Como se mencionaba anteriormente, el bullying puede tomar diferentes formas de manifestaciones:

- Intimidaciones verbales,
- Intimidaciones psicológicas,
- Agresiones físicas,
- Aislamiento social,
- Acoso sexual,
- Ciberbullying.

Si desmenuzamos más profundamente los datos que tenemos, podemos encontrar las siguientes conclusiones sobre el acoso escolar:

- Fenómeno psicosocial complejo con implicaciones serias y alto impacto en el proceso educativo;
- Es un fenómeno cultural y no natural, puesto que la violencia, como veíamos anteriormente, es una conducta aprendida;
- Compromete la dimensión del desarrollo moral de quienes en él participan, no rompe una convención social, sino el fundamento de la convivencia y la conformación de la sociedad;
- Existe una dimensión socio-jurídica, ya que se presenta un ataque sistemático y constante a los derechos inherentes al ser humano.

Ciberbullying

En el transcurrir del documento hemos hablado de la importancia del ciberespacio y sus usos en la actualidad. Tomando en cuenta el tema de la agresión, vemos que los usos malintencionados que hemos descubierto en los diferentes modos de interacción de los usuarios, como serían el phishing, scam, bulo, sexting y grooming entre otros,

corresponderían a una agresión instrumental, pues tienen la finalidad de conseguir un fin perjudicial para el usuario, logrando un beneficio propio por parte del agresor.

Por ello no es casualidad que en los últimos años, se escuche en noticieros de hackeos a grandes empresas donde se exigen grandes sumas de dinero a cambio de no revelar información importante, asimismo se conoce de nuevos sistemas de seguridad ante posibles amenazas cibernéticas y demás. En redes sociales se escucha y se sabe de videos e imágenes sobre adolescentes que son agredidos y humillados y es cada vez más alarmante ver el aumento de las cifras. Con la era tecnológica, el fenómeno del ciberacoso ha adquirido presencia a nivel mundial pues se trata de una nueva forma de violencia que se investiga en los últimos años debido al número de casos reportados y por la repercusión que tiene en la vida de las personas y en la sociedad, pero ¿qué se está haciendo para velar por la seguridad de chicos y grandes en Internet?

En México, con el fin de generar información estadística que permita tener una primera aproximación al fenómeno del ciberacoso y su impacto en la población afectada, el InstitutoNacional de Estadística y Geografía (INEGI) realizó en 2017 el levantamiento del "Módulosobre Ciberacoso" (MOCIBA) dentro de la "Encuesta Nacional sobre Disponibilidad y Uso de las TIC en Hogares" (ENDUTIH) donde se aborda este tema que es una forma de victimización relativamente reciente y que se ha magnificado a partir del uso intensificado de internet, el teléfono móvil y en general de las tecnologías de la información.

Los principales resultados exhibidos en 2019, son los siguientes:

- La población total mexicana, de los 12 a 59 años, corresponde a 84.5 millones de personas;

- La población de 12 a 59 años de edad que usa Internet es de 73%

- El 16.8% de dicha población, **ha experimentado por lo menos alguna situación de ciberacoso,** teniendo una prevalencia hacia las mujeres de 1.7%

- Respecto a la población "acosada", el **20.1% corresponde al rango de edad entre 12 y 19 años** (adolescentes y jóvenes).

- **En el ámbito escolar, el 19% de la población en nivel básico está en riesgo de sufrir acoso/abuso por medios electrónicos.**

- Las entidades federativas con mayor impacto en esta problemática corresponden a:

- Tabasco, 22.1%
- Veracruz, 21.8%
- Zacatecas, 21.4%
- Guanajuato, 20.3%
- Aguascalientes, 20.3%

● Las situaciones experimentadas registradas corresponden a:
- Mensajes ofensivos, 40.1%
- Contacto mediante identidades falsas, 31.4%
- Llamadas, 27.5%
- Provocaciones para reaccionar de forma negativa, 25%
- Insinuaciones o propuestas sexuales, 22.6%
- Rastreo de cuentas o sitios web, 20.3%
- Recibir contenido sexual, 19.7%
- Suplantación de identidad, 19.4%
- Criticas o burlas por apariencia o clase social, 11.8%
- Publicación de información personal, 10.3%

El 54% de la población de 12 a 59 años de edad que declaró haber vivido ciberacoso, experimentó más de una situación de las diez consideradas; mientras que el 46% experimentó solo una de ellas.

● Porcentaje de la población que sufrió ciberacoso, según la identidad del agresor
- Conocido, 41.2%
- Desconocido, 58.8%

● Porcentaje de la población que vivió ciberacoso y conoce al agresor, según cercanía
- Ex novio, ex pareja o familiar, 22.3%
- Amigo, 32.7%
- Compañero de clase/trabajo, 22.8%
- Conocido de poco trato o solo de vista, 46.4%

● El efecto causado tras haber recibido ciberacoso es el siguiente:
- Enojo, 66.9%
- Desconfianza, 43.2%
- Inseguridad, 29.3%
- Frustración, 22.5%
- Miedo, 22.3%
- Estrés, 22.2%
- Nervios, 20.2%
- Nada, 10.8%
- Otro, 4.3%

- Las principales formas de solución que los usuarios han buscado:
    - Bloquear a la persona, cuenta o página, 60.1%
    - Ignorar o no contestar, 27.7%
    - Eliminar la publicación, mensaje o video, 20.1%
    - Cambiar o cancelar no. de teléfono, cuenta o contraseña, 18.5%
    - Informar a una persona, 13.9%
    - Hablar con el agresor, 11.1%
    - Denunciar ante ministerio, policía o proveedor del servicio, 5.4%
    - Otra acción tomada, 5.4%
- Las medidas de seguridad que se tomaron para proteger equipos o cuentas:
    - Crear o poner contraseñas (claves, huella digital, patrón, etc), 90%
    - Instalar o actualizar programas antivirus, contrafuegos o antiespías, 47.6%
    - Cambiar periódicamente las contraseñas, 21.5%
    - Bloquear ventanas emergentes del navegador, 19.7%
    - No abrir ni guardar archivos que envían personas desconocidas, 18.7%

Con estos datos podemos inferir lo siguiente:

- Que de la población acosada, el 20.1% sean jóvenes y adolescentes, alarma en el grado de atención que hay que brindar tanto a víctimas, como a acosadores para preparar y aplicar programas de prevención y acción adecuados a las necesidades de esta población;

- Reforzando el punto anterior, que el 19% de la población escolar en educación básica se encuentre expuesta a ser víctima de ciberacoso, nos permite vislumbrar la necesidad de actuar con prontitud, cautela y precisión, ya que la educación básica va de la mano a una de las etapas más importantes para la conformación de la identidad del ser humano;

- Por el impacto que el ciberacoso tiene en las entidades federativas, se comprueba que estamos frente a una **problemática cultura** l;

- Dejando de lado a los desconocidos, los porcentajes más elevados respecto identidad del agresor, corresponden a conocidos de poco trato y amigos, poniendo al descubierto la incidencia de la **agresión horizontal**.

Recuperado de http://www.beta.inegi.org.mx/contenidos/proyectos/investigacion/ciberacoso/2015/doc/mociba2015_principales_resultados.pdf el 14 de julio de 2017.

Por ello, es necesario ahondar en el conocimiento del tema, así como varios gobiernos e instituciones de diferentes países lo han hecho, destacando Canadá, Reino Unido, España y Estados Unidos, quienes han actuado como resultado de los daños y perjuicios que se componen en distintos aspectos de la salud mental y física de las víctimas.

En la mayoría de estudios sobre violencia escolar, las TIC's aparecen como factor interviniente en el origen de las situaciones violentas, quedándonos en una visión parcial de esta realidad, ya que éstas pueden ser además, el medio, lugar o escenario de las distintas formas de acoso u hostigamiento entre iguales (Hernández & Solano, 2007).

Uno de los pioneros en este tema y en la definición del concepto es Bill Belsey, un educador canadiense que dice lo siguiente: *"El ciberacoso implica el uso de tecnologías de información y de comunicación para el comportamiento deliberado, repetitivo y hostil de una persona o un grupo con el fin de hacerle daño a otro/s"*[11]. Dicho concepto es retomado también en la página estadounidense "Cyberbullying Research Center" que es una plataforma virtual dedicada única y exclusivamente al tema del ciberbullying.

Sin embargo, Parry Aftab, investigadora estadounidense considera ***ciberbullying cuando un niño o un adolescente es atormentado, amenazado, acosado, humillado, avergonzado o se convierte en el blanco de otro niño, niña, o adolescente a través de Internet, tecnologías interactivas y digitales o teléfonos móviles***. Tiene que implicar a un menor de edad en ambos lados, ya que cuando un adulto está involucrado no es ciberbullying, sino otra forma de ciberacoso.

Aftab diferencia entre dos formas de acoso; directo e indirecto. El **acoso directo** es el envío de mensajes directos a otros niños o adolescentes; mientras que el **acoso indirecto o por delegación** implica utilizar a otras personas para acosar cibernéticamente a la víctima, ya sea con o sin el conocimiento de estos cómplices. El acoso indirecto puede ser más peligroso ya que puede incluir a personas adultas en el hostigamiento. La mayoría de las veces, son cómplices no deliberados y no saben que están siendo utilizados por el/ la ciberacosador/a.

Por lo tanto podemos clarificar la información de la siguiente manera:

Ciberacoso	Ciberbullying
Engloba **diferentes formas de acoso** a través del uso deliberado de las TIC's.	Se despliega como **una variable** de acoso cibernética.
Las edades de las personas involucradas pueden variar entre **niños y adultos sin distinción**, por ello surge el hackeo, grooming y sexing, entre otros.	Su principal característica es que el acoso se da **entre pares** (personas en el mismo rango de edades): niños, adolescentes o jóvenes.

De forma general, se considera la existencia de dos modalidades del Ciberbullying:

[10] Recuperado de http://www.cyberbullying.ca/ el 24 de julio de 2017.

1. Aquél que surge como reforzamiento de un bullying ya emprendido;
2. Aquél acoso entre iguales a través de las TIC's sin antecedentes.

La primera se considera una forma de acoso escolar más sofisticada, desarrollada generalmente cuando las formas de acoso tradicionales ya no brindan al agresor la satisfacción necesaria y busca algo más atractivo, de esta forma, los efectos que genera se suman a los ya creados anteriormente y puede amplificar incluso los daños debido a la generalización del acoso a través de las páginas web. Existe una relación previa de "cara a cara". Esta es la modalidad a la que más nos vamos a enfrentar en instituciones educativas. Comportamientos de exclusión y aislamiento en los espacios físicos son los más habituales como previos y añadidos, a las experiencias en contextos virtuales.

La segunda modalidad implica que sin precedente alguno, el adolescente comience a recibir diversas formas de hostigamiento por pares a través de las tecnologías de información y comunicación. Víctima y agresor pueden no tener contacto o conocimiento de uno y otro, pero puede el agresor en ocasiones, propiciar el encuentro.

Al igual que en el acoso escolar, en el ciberbullying prevalece la desigualdad de poder entre víctima y agresor, pero tiene las siguientes características específicas:

- Exige el dominio y uso de las TIC's;
- Recoge diversos tipos o formas de manifestar el acoso a través de las TIC's;
- Efecto desinhibidor sobre los comportamientos, propiciando actuar impulsivamente mediante las TIC's;
- Sentimiento de invencibilidad en línea y reducción de las restricciones sociales, así como dificultad para percibir el daño causado;
- El desconocimiento del agresor intensifica el sentimiento de impotencia e imposibilita un posible acercamiento empático entre ambos actores;
- Acceso 24/7 a la víctima, junto con una viralidad y audiencia ampliada;
- El acoso invade ámbitos de privacidad y aparente seguridad como el hogar y la familia, promoviendo un sentimiento de completa desprotección;
- El acoso puede hacerse público, abriendo la oportunidad a que más personas participen de éste;
- Puede permitir el acoso indirecto.[12]

[11] María Hernández, I. Solano "Cyberbullying, un Problema de Acoso Escolar, Revista AIESAD, 2007.

Los diferentes medios que se tienen identificados para llevar a cabo el ciberacoso, son los siguientes: el correo electrónico, el teléfono móvil, la mensajería instantánea, páginas web y redes sociales; mientras que los tipos de agresiones, de acuerdo a las investigadoras Kowalski, Limber y Agatston, se pueden dividir de la siguiente forma:

1. **Insultos electrónicos**: Intercambio breve y exaltado entre dos o más personas, que tiene lugar a través de alguna de las nuevas tecnologías. Reciprocidad de e-mails privados o en contextos públicos como chats, con intercambio mutuo de insultos entre varias personas implicadas.

2. **Hostigamiento**: Mensajes ofensivos frecuentes a la persona elegida como blanco por correo electrónico, en foros públicos como salas de chat y foros de debate; envío de cientos o miles de mensajes de texto al teléfono móvil de la persona. A diferencia de los insultos es a largo plazo y unilateral, incluyendo en ocasiones a más de un ofensor frente a una única víctima.

3. **Denigración**: Información despectiva y falsa respecto otra persona que es publicada en una página web o difundida vía e-mails o mensajes instantáneos, por ejemplo fotos de la víctima alteradas digitalmente, sobre todo de forma que refleje actitudes sexuales o que puedan perjudicar a la persona en cuestión.

4. **Suplantación**: El acosador se hace pasar por víctima, la mayoría de las ocasiones utilizando la contraseña de ésta para acceder a sus cuentas electrónicas y con ello enviando mensajes negativos, agresivos o crueles a otras personas como si hubiesen sido enviados por la propia víctima.

5. **Desvelamiento y sonsacamiento**: Consiste en revelar información comprometedora de la víctima sin su consentimiento a otras personas enviada de forma espontánea y después difundida a otras personas. Involucra el sexting.

6. **Exclusión**: No dejar participar a la persona de una red social específica.

7. **Ciberpersecución**: Envío de comunicaciones electrónicas reiteradas hostigadoras y amenazantes por distintos medios electrónicos.

8. **Paliza feliz (happy slapping):** Es cuando se realiza una agresión física a una persona a la que se graba en vídeo con el teléfono celular y luego se publica en la red para que lo vean miles de personas. (Garaigordobil, 2011)

Actores involucrados

Ya que hemos revisado cómo se da el flujo del ciberacoso, así como las formas en que se lleva a cabo, es importante identificar a aquellos participantes que se encuentran alrededor del fenómeno, puesto que se constituye una dinámica de juego de roles que rebasa la acción individual. Para que dicha dinámica se mantenga, los involucrados aportan una representación o papel que perpetúa la existencia de la conducta. En ocasiones, una sola persona, puede ocupar a la vez varios "papeles" dentro de la dinámica del ciberbullying.

AGRESORES

También llamados bullys o abusadores, son los responsables directos de la agresión, quienes la provocan y la inician. Puede ser únicamente un agresor, o bien un grupo de varios adolescentes que actúen en conjunto o cada quien por su parte, pero con el mismo objetivo de dañar a la otra persona. Generalmente tienen un perfil con las siguientes características:

- Poseen cierta jerarquía de poder (incluida una mayor competencia tecnológica) o prestigio social sobre las víctimas y con ella buscan imponer o dominar;
- No cuentan con un buen manejo de habilidades sociales, ya sea porque lo hacen de forma negativa o porque carecen de ellas y prefieren atacar a su víctima de forma indirecta, en vez de cara a cara;
- Gustan de dañar a otra persona y carecen de empatía;
- Poseen una tendencia clara de emplear fácilmente la violencia reactiva como instrumental a través de medios electrónicos;

Cuando se da el caso de continuidad del bullying ahora en ciberbullying, generalmente se suman también las siguientes características:

- Tienen una gran dificultad para asumir y cumplir la normatividad;
- Personas comúnmente más conflictivas y belicosas que la media de sus compañeros, destacan por una personalidad fuerte y definida. Suelen ser agresivos no sólo con compañeros, sino también con maestros y autoridades en general;
- Utilizan la agresión instrumental como medio de solución de conflictos. No ceden en negociaciones, ya que sus objetivos son los únicos que deben alcanzarse sin importar los medios. Tienen poca tolerancia a la frustración.

Cabe mencionar que la intención de causar daño de forma explícita no está siempre presente en los inicios de la acción agresora. El impacto y recorrido de este tipo de acciones (sean claramente intencionadas **o derivadas de una broma sin aparente deseo de causar perjuicio**) es difícil de medir y cuantificar.

Pueden clasificarse en activos y pasivos o llamados también seguidores o cómplices, pues estos últimos sin iniciar la agresión, la alientan y dan muestras de simpatía al agresor.

VÍCTIMAS

Son las personas que sufren los ataques directos del agresor/es. Normalmente poseen una percepción sumamente negativa de sí mismos, negando sus habilidades y aptitudes como persona insistiendo en que son “estúpidos”, “fracasados”, “faltos de atractivo” y constantemente se avergüenzan de sí mismos frente a otros. Tienden a ser introvertidos y con un nivel bajo de autoestima, el cual se ve reforzado negativamente durante y después del acoso. De acuerdo a María Ángeles Hernández e Isabel María Solano, doctoras en Pedagogía y profesoras en la Universidad de Murcia, existen tres tipos de víctimas:

- Víctima típica: Quien recibe los ataques sin lograr defenderse de forma alguna;
- Víctima provocadora: Quien tiene dificultad para relacionarse con sus compañeros y que dicha condición es aprovechada por los agresores para dañarlo. Se defiende buscando el enfrentamiento.
- Víctima agresora: Quien sufre agresiones de algunos y luego es agresor de otros a los que considera más débiles que él/ella.

El ciberbullying conlleva una serie de **consecuencias** que tienen un impacto en los menores a nivel **psicológico, social y educativo**. La aparición de alguna de ellas podría ser motivo de sospecha:

- **Cambios físicos y emocionales**: Constantes manifestaciones de dolor (por ejemplo: de cabeza o estómago), alteraciones del estado de ánimo, principalmente de humor: momentos de tristeza, apatía e indiferencia; síntomas de ansiedad, estrés o signos inusuales de comportamiento agresivo.
- **Cambios de conducta/sociales**: Modificaciones en sus actividades de ocio habituales, en su relación con adultos, en cuanto a frecuencia y dependencia de ellos, en la cantidad de comida y maneras de comer, en los hábitos de sueño, **de improvisto deja de usar el ordenador y el teléfono**, variaciones repentinas en los grupos de amigos, en ocasiones antagónicos; autolesiones, amenazas o intentos de suicidio.
- **Cambios en el contexto académico**: El adolescente se ve involucrado en incidentes dentro de la escuela, se reduce su capacidad de concentración y de mantenimiento de la atención, altibajos en los tiempos de estudio y el rendimiento escolar, pérdida de interés en la escuela, pérdida y/o deterioro de pertenencias físicas, lesiones físicas frecuentes sin explicación razonable. [13]

TESTIGOS

Son las personas que atestiguan en redes sociales las agresiones que se dan hacia la o las víctimas por parte del agresor/es. A pesar de contar con un ambiente más cerrado, pueden estar o no presentes, de forma física, en el momento de la creación del comentario, video, carga de fotos y demás que dan paso al ciberbullying. Tienen un papel muy importante en ésta dinámica ya que pueden participar de diferentes formas, de acuerdo a las siguientes definiciones:

- Testigos activos: Quienes apoyan de manera directa o indirecta al agresor o a sus cómplices. En redes sociales y otros medios se presentan a favor el agresor;
- Testigos pasivos: Quienes aparecen en silencio alrededor del suceso como actores neutrales. Con el paso del tiempo, su indiferencia será un fuerte reforzamiento

[12] Red.es, “Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad”, Gobierno de España.

para el agresor. Al recibir material de acoso distribuido masivamente, no hacen nada, ni denuncian el hecho;

- Testigos prosociales: Quienes intentan por cualquier medio detener el acoso e incluso apoyar abiertamente a la víctima sin agredir instrumentalmente al agresor, tienen sentimientos de empatía y solidaridad con la víctima. No reenvían el material, censuran, bloquean y/o reportan a la red social lo ocurrido, buscan ayudar a la víctima.

"Todos como usuarios y receptores de mensajes, visitantes de redes, chats, foros, podemos en un momento de consulta, de reenvío y etiquetación de algún mensaje o sitio de votación convertirnos en testigos de ciberacoso".

Asociación Mexicana "Yo Lo Borro"[14]

Consejos contra el ciberbullying

Puesto que ya hemos hablado de las formas en que el ciberacoso se hace presente e incluso de las consecuencias que se presentan, nos encontramos ante las preguntas y respuestas más esperadas ¿qué hacer cuando ya estamos frente a uno de estos casos? y ¿cómo prevenirlo? Por ello ahondaremos en estas dos dimensiones desde las cuales podemos actuar frente a éste fenómeno.

Para evitar exponerse en la medida de lo posible a situaciones de ciberbullying, es mejor tomar precauciones que desglosaremos en recursos para cada estrato poblacional involucrado en la dinámica: alumnos, padres y madres de familia, y maestros; así como la importancia del manejo de datos sensibles por parte de los adolescentes.

Manejo de datos sensibles

Ya bien sabido es que los adolescentes utilizan el internet de forma cotidiana, prácticamente 24/7, ya sea desde los teléfonos móviles, las tabletas electrónicas o desde la máquina de cómputo. Como mencionábamos, dentro de sus hábitos frecuentes,

[13] Recuperado de: http://www.camaleonbox.com/roles-ciberbullying/ el 24 de julio de 2017.

además de la búsqueda de información, se encuentran el uso de las redes sociales como Instagram, Snap Chat, Twitter, Facebook, entre otros; las plataformas como YouTube y la mensajería instantánea, como Whatsapp. La principal medida de concienciación es la salvaguarda de su identidad digital y de la información que comparten con ella.

IMPORTANCIA DE LA PROTECCIÓN DE IDENTIDAD

Por identidad entendemos el "conjunto de rasgos o informaciones que individualizan o distinguen algo y confirman que es realmente lo que se dice que es" (RAE), de tal forma que la ***identidad digital*** hace referencia al cúmulo de rasgos que caracterizan a un individuo o colectivo en un entorno tecnológico, por lo tanto estar en la red implica contar con la representación de uno mismo y se va construyendo con los insumos que aportamos o compartimos en dichos medios, por ejemplo los textos, imágenes, videos, notas y más, y así al ser percibido subjetivamente por los demás usuarios, se va conformando una ***reputación tecnológica***. La homogeneidad entre ambas identidades puede o no ser la misma; sin embargo, para gozar de un entramado social más estable, una vida más activa y sana, se recomienda que ambas identidades compaginen.

Precisamente porque hablamos de una identidad en el ámbito tecnológico, es que debe cuidarse la **seguridad** de ésta. Uno no va por la calle dando copias de las llaves de su casa al que se encuentre en el camino, lo mismo pasa con las contraseñas de cuentas electrónicas, ya sean de correos, redes sociales o datos bancarios, no se comparten a los demás.

El tema de la **visibilidad** en internet es un tema amplio que podemos resumir de la siguiente forma: Toda actividad que genera un individuo en la red, la cual puede ser positiva o negativa. Puede ser autoconstruida por medio de los *posts*, mensajes, comentarios, video, fotos y demás; pero puede ser también fruto de referencias o comentarios de terceros. Esta visibilidad hace referencia a qué tanto es uno conocido o popular en el medio. Es importante preguntarse si uno busca ser visible o no. Puede medirse, por ejemplo, a través de los *likes*, o cantidad de seguidores en las cuentas de redes sociales.

Aunado a estos temas, se encuentra también el de la **privacidad, probablemente el más importante en este ámbito digital**, pues su relevancia radica en la consciencia del cuidado

de los datos personales en internet y el uso que puede hacerse con ellos, ¡he ahí la clave principal para la toma de decisiones! Es necesario incidir en que uno como usuario, es quien expone de forma voluntaria sus datos en estas redes, como: dirección de correo electrónico, fotografías, teléfono, preferencias políticas y religiosas, currículum profesional, gustos por música, lectura y demás, los cuales son campos comunes al momento de la creación de un nuevo perfil; sin embargo, tanto por las conductas ilícitas electrónicas mencionadas al inicio del documento, como por otro tipo de rastreo de información, estos datos pueden ser expuestos por los mismos sitios o por terceros. Los proveedores de estos servicios ya pueden guardar información como el número de IP (número que identifica un dispositivo en una red en internet) o sobre el tráfico (intercambio) de datos durante la conexión y utilizarlas para fines desconocidos o simplemente para análisis de datos y mercadeo.

Algunas recomendaciones para el cuidado de identidad, privacidad de datos, visibilidad y creación de una buena reputación digital, son:

- Para asuntos personales o privados, utilizar siempre una cuenta privada; evitando no usar la de una empresa, institución educativa o club.
- Acudir al uso de "nicknames" para la identidad virtual, protegiendo datos personales como nombre completo, dirección y datos de contacto.
- Cuidar el lenguaje que se utiliza y los contenidos a compartir, ya que va generando reputación digital y al siempre quedar un registro en internet, será poco posible eliminar cosas que uno no haya querido publicar: insultos, imágenes propias o de terceros, bromas a compañeros, contenido no deseable.
- Cuidar los sitios o páginas de internet que se visitan, ya que genera "historial" y con ello la gente te podrá identificar.
- Cuidar las *net-etiquetas*, que son normas de comportamiento en el medio virtual y que están directamente relacionadas con las normas morales.
- Tener una contraseña de varios caracteres (alrededor de ocho), los cuales puedan alternarse entre mayúsculas, minúsculas, números y, de poderse, signos; aumentando así el grado de dificultad para quien busque adquirir la contraseña.
- Tener más de una contraseña para las diferentes cuentas, así evitas que al conseguir la única que tienes, dé acceso a todas las demás cuentas electrónicas.

Con ello lograrás evitar también el robo o suplantación de identidad, robo de datos bancarios y de dinero.

Recursos de prevención para alumnos

1. **Prepárate**. Navegar por internet es como un viaje: conviene saber qué maravillas puedes descubrir, pero también qué peligros puedes encontrar en el camino.
2. **Iniciación**. Navegar por internet es como moverse por una gran ciudad: es fácil perderse. Así que si vas a empezar a navegar por internet hazlo en compañía de un adulto.
3. **Espíritu crítico**. Navegar por internet es como escuchar un rumor: si tú ves o lees algo que puede no ser cierto, debes contrastarlo con otras fuentes, es la mejor manera de salir de dudas.
4. **Mecanismos de control**. Navegar por internet es como abrir una ventana: Puedes mirar al exterior, pero también pueden verte desde el otro lado. Infórmate sobre los medios de control que hay para que seas tú quien decide lo que quieres mostrar a los demás.
5. **Seguimiento**. Navegar por internet es como caminar por suelo mojado: siempre dejas huella por donde pasas. Así que recuerda que todo lo que haces en la red queda registrado en alguna parte.
6. **Denuncia**. Navegar por internet es como ir por la calle: si eres testigo de una agresión o de un comportamiento criminal, denúncialo, es tu responsabilidad.

	Policía Cibernética de la Comisión Nacional de Seguridad	**Policía Cibernética en la Ciudad de México**
Teléfono 24/7	5242-5100, ext. 5086	088
Twitter	@CEAC_NS	@UCS_CDMX / #CiberneticaCDMX
Mail	ceac@cns.gob.mx	policia.cibernetica@ssp.df.mx

7. **Privacidad**. Navegar por internet es como tener una caja fuerte: Si vas dando la combinación a todo el mundo, cualquiera podrá ver lo que guardas dentro. Así que no compartas tu contraseña con nadie ni tampoco tu información personal.
8. **Virtualidad / Realidad**. Navegar por internet es como estar en carnavales: Cualquiera puede llevar un disfraz y ocultar su verdadera identidad. Si te citas con alguien a quien sólo conoces por internet, hazlo siempre acompañado de un adulto de tu confianza.

9. **Fraude / Engaño**. Navegar por internet es como comer sano: antes de clavar el diente a algo, asegúrate que no te hará daño. En internet hay páginas y enlaces que pueden ser perjudiciales para tu seguridad y ordenador.
10. **Espacio en común**. Navegar por internet es como ver la tele: Aunque tengas una en cada cuarto, lo ideal es sentarte con los tuyos y disfrutar de la tele todos juntos.[15]

Recursos de prevención para padres y madres de familia

"Tomamos la mano de nuestros hijos cuando cruzamos la carretera, hablamos con ellos sobre el peligro de hablar con extraños. Y luego les damos una computadora y los dejamos solos. Ya no podemos fingir que no sabemos sobre el lado oscuro de internet".

Roger Merrick, policía canadiense.

Puesto que es muy probable que los menores se acerquen a adultos de confianza, principalmente padres y madres de familia, estos deben estar preparados para enfrentarse también a este fenómeno desde antes de que se presente, por ello dejamos algunas recomendaciones para los adultos:

1. **Infórmate**. Conoce los medios y usos que se le puede dar a la tecnología y las redes sociales con anticipación. Enséñale a tu hijo el uso correcto y prevenlo de peligros.
2. **Horarios y acompañamiento**. Establece horarios en casa para el uso de aparatos electrónicos y la navegación en internet a través de redes sociales y otras páginas. Procura en la medida de lo posible estar al pendiente del uso.
3. **Verifícalo**. Siempre corrobora la información que veas y las fuentes. Transmite esto a tu hijo.
4. **Asegúrate**. Infórmate sobre los medios de control que hay para que seas tú quien decida lo que quieres mostrar a los demás y a la vez puedas transmitirlo a tu hijo/a.
5. **Precaución**. Ten precaución con lo que tu hijo y tú publican o comparten, todo lo que se sube a internet, aunque se elimine, deja registro en algún lado de la red.

[14] Extraído del video "Diez formas de prevenir el #Ciberacoso" de la página oficial de Facebook de CanalSur Radio y Televisión; Andalucía, España. Publicado el 20 de Junio de 2017.

6. **Privacidad**. No compartas información personal en internet, como nombre completo, edad, dirección, ubicación actual, datos bancarios y menos tu contraseña. Enséñalo a tu hijo.
7. **Denuncia**. Enseña a tu hijo que si ve actos, comentarios, o agresiones de un compañero a otro, lo denuncie a sus maestros, en la red social y de ser necesario a:
8. **No hablar con extraños**. Al igual que en la calle, enseña a no aceptar a personas desconocidas en sus redes sociales y menos verse con ellos en persona.
9. **Confianza**. Siempre inspira confianza a tu hijo a través de la comunicación, para que te platique cualquier situación que pueda ser perjudicial para él/ella o sus compañeros.
10. **Concepto del delito**. Enséñales que las conductas que llevan a cabo en el uso de las nuevas tecnologías e internet también tienen consecuencias en el ámbito familiar (castigos), escolar (sanciones), o en casos más graves, incluso penales (delitos).

Recursos de prevención para maestros

Finalmente y no menos importante, está el trabajo que los maestros harán en tema de prevención dentro del aula, que consiste en reforzar las recomendaciones ya dadas a los padres y madres de familia:

1. **Infórmate**. Conoce los medios y usos que se le puede dar a la tecnología y las redes sociales con anticipación. Enséñale a tu alumno el uso correcto y prevenlo de peligros.
2. **Horarios y acompañamiento**. A menos que tu clase lo requiera y apegado a las reglas de la escuela, no permitas el uso de aparatos electrónicos y redes sociales durante clase. Procura estar pendiente de su uso durante recesos.

3. **Verifícalo**. Siempre corrobora la información que veas y las fuentes. Transmite esto a tus alumnos.
4. **Asegúrate**. Infórmate sobre los medios de control que hay para que sean los alumnos y sus padres quienes decidan lo que quieren mostrar en internet y redes sociales.
5. **Precaución**. Recuerda a tus alumnos que todo lo que se sube a internet, aunque se elimine, deja registro en algún lado de la red.
6. **Privacidad**. No compartas información personal en internet, como nombre completo, edad, dirección, ubicación actual, datos bancarios y menos tu contraseña. Enséñalo a tu alumnos.
7. **Denuncia**. Enseña a tu alumno que si ve actos, comentarios, o agresiones de un compañero a otro, lo denuncie a sus maestros, en la red social y de ser necesario a:
8. **No hablar con extraños**. Al igual que en la calle, enseña a tus alumnos a no aceptar a personas desconocidas en sus redes sociales y menos verse con ellos en persona.
9. **Confianza**. Siempre inspira confianza a tus alumnos, para que te platiquen cualquier situación que pueda ser perjudicial para él/ella o sus compañeros.
10. **Concepto del delito**. Enséñales que las conductas que llevan a cabo en el uso de las nuevas tecnologías e internet también tienen consecuencias en el ámbito familiar (castigos), escolar (sanciones), o en casos más graves, incluso penales (delitos).

Cómo actuar

Cuando ya estamos ante una situación de ciberbullying, la principal ayuda a brindar será siempre para el adolescente inmerso en los ataques, la víctima, por lo cual brindamos estos 8 pasos a seguir:

1. **Pedir ayuda**. El menor de edad, al estar en una situación de ciberbullying, debe acercarse a sus padres o en su defecto a una persona adulta de confianza, asegurándose de que la persona conoce y entiende las pautas para que ambos puedan ir en el mismo sentido y para que en su ánimo de protección, no haga cosas que terminen siendo perjudiciales.
2. **No responder a las provocaciones**. Ya que no sólo no ayuda en nada, sino que en vez de calmar la situación, será un motivo más para que el acosador continúe con la hostigación.
3. **No hacer presunciones**. Puesto que ni las circunstancias ni las personas que parecen implicadas pueden ser lo que aparentan, es mejor mantener un margen de duda razonable para no actuar con bases equivocadas y aumentar el problema.
4. **Revisar y modificar información pública sensible**. Lo mejor será eliminar toda la información sensible como datos de contacto, direcciones y demás que pueda seguir siendo material para continuar con el ciberacoso, así como de los contactos que tiene acceso a esta información a los perfiles. Una buena opción será la de cambiar las contraseñas de redes sociales y demás, así como revisando los aparatos electrónicos en que uno se conecta, para eliminar la existencia de malwares.
5. **Guardar las pruebas del acoso**. Ya sea con capturas de pantalla o la impresión de correos electrónicos o cualquier otro material utilizado para el acoso, puesto que pueden servir de pruebas o bien para conocer sobre la posible identidad del agresor (si se hace de forma anónima).
6. **Comunicar a quienes agreden**, por el mismo medio, **que se está molesto con dichos actos,** pero sin caer en amenazas ni agresiones. Recordarles también que lo que los agresores realizan, es perseguible por la ley.
7. **Denunciar en el medio digital.** Puesto que las páginas oficiales cuentan con esta opción, es importante que la víctima pueda reportar el caso a las redes sociales en que se realiza el acoso.
8. **Si la persecución persiste, tomar medidas legales**. Ya que de no frenarse los actos por los agresores, sí será necesario acudir al departamento legal encargado de estos casos. [16]

[15] Recomendaciones adaptadas del "Decálogo para una víctima de ciberbullying por Pantallas Amigas, España. Recuperado en http://www.ciberbullying.com/cyberbullying/2010/09/01/decalogo-para-una-victima-de-ciberbullying/ el 24 de julio de 2017.

Ahora bien, los adultos deben transmitir a los menores la confianza suficiente como para que recurran a uno en caso de presentarse el ciberacoso, para ello, dejamos estos pasos, retomados de Jorge Flores Fernández, colaborador experto en ciberacoso para "Pantallas Amigas, España":

- No reaccionar de forma brusca. Hay que prestar atención a la gravedad y frecuencia del acoso (para tratar de calibrar su magnitud), así como a la manera en que la víctima lo sufre. Apoyar al menor es lo primero para que remita su angustia. Luego llegará el momento de actuar.
- Cuando se dan amenazas graves de daño físico directo el tema debe tomarse muy en serio, máxime cuando se sabe que quien acosa dispone de datos personales como dirección o centro escolar. Recurrir a la policía no está de sobra en estos casos.
- Si hay víctimas, es porque hay abusones, y no es fácil identificarlos, siquiera en la propia casa. Es bueno contar a los menores que esas acciones causan un daño real y constituyen un delito.

Revisión general de programas de éxito en iniciativas de intervención

Campaña "Ponle cara a tu face" México.

Nombre: Ponle cara a tu face.
Creadores: Fundación en Movimiento A.C.
Objetivo: Volver a darle valor, respeto y responsabilidad a lo que decimos y hacemos, evitando así la comunicación irresponsable y ofensiva, ya que es un atentado contra la dignidad de las demás personas.
Población objetivo: Estudiantes desde 1o de primaria hasta 3o de preparatoria.
Tiempo de trabajo: Un ciclo escolar.
Metodología:

Se busca implementar una campaña de respeto en los tres niveles participantes de las escuelas, donde a través de pláticas salón por salón, se explica, ejemplifica y aplica el tema

principal: RESPETO, aterrizado específicamente al uso de las redes sociales. Al terminar la plática, los alumnos:

- Hacen un pacto donde se comprometen a no volver a poner en ningún medio electrónico interactivo (chat, red social, e-mail, mensaje de texto de celular, páginas de chisme y demás) ninguna frase o comentario que no esté dispuesto a sostener cara a cara con la otra persona; así como el evitar publicar argumentos o elementos ofensivos como:
    - Groserías (aunque no se digan a alguien en especial),
    - Ligas de pornografía,
    - Fotos personales o de otros en escenas comprometedoras.

Denunciar a las personas que realicen un mal uso de los medios electrónicos interactivos de la siguiente manera:

- Con el proveedor de la página (Facebook, Twitter, Skype..) que cuenta con un formato para ello,
- En la Secretaría de Seguridad Pública.

Los maestros y los encargados de disciplina (prefectos, tutores escolares) y en su caso los psicólogos, quienes también toman las pláticas, se hacen responsables de dar seguimiento al cumplimiento del pacto de cada salón, así como a casos específicos, con la disponibilidad de consultar al personal de Fundación en Movimiento A.C. y de la campaña "Ponle cara a tu face".

El Método KIVA contra el Bullying y Cyberbullin. Finlandia

Nombre: Método KiVA
Creadores: Universidad de Turku, Finlandia, a cargo de equipo liderado por Tina Mäkela y Christina Salmivalli.
Objetivo: Prevenir y enfrentar el bullying y ciberbullying en los colegios.
Población objetivo: Estudiantes de entre 7 y 15 años de 234 instituciones educativas.
Tiempo de trabajo: Ciclo escolar de 2009.
Metodología:

El Método KiVA, por sus siglas en finlandés: "Kiusaamista Vastaan" (contra el acoso escolar) surge en 2009 como un compromiso entre la comunidad educativa y el gobierno finlandés (siendo el mayor estudio realizado en dicho país) a través de la Universidad de

Turku y la financiación del Ministerio de Educación y Cultura de Finlandia, para la investigación, prevención y enfrentamiento del acoso escolar en los colegios. Se realizó una gran prueba controlada y aleatoria de 117 colegios con intervención y 117 de control resultando en un total de 150,000 alumnos.

El objetivo de prevenir y enfrentar el acoso y ciberbullying lo hacen a través de la concientización sobre la importancia de las acciones del grupo, así como empatizar, defender y apoyar a la víctima, ya que descentraliza la atención en el binomio agresor y víctima, dirigiendo el programa principalmente a los testigos.

El programa se basa en tres pilares base: Prevención, intervención y seguimiento. Los estudiantes reciben 20 clases a los 7, 10 y 13 años para reconocer las distintas formas de acoso y mejorar la convivencia. Se realizan 10 lecciones y trabajos durante el ciclo escolar sobre el respeto a los demás y la empatía. En cada colegio hay un “equipo KiVa”, formado por tres adultos que se ponen a trabajar en cuanto tienen conocimiento de un caso de acoso escolar o ciberbullying en el centro. Primero actúan como filtro, para reconocer si es un acoso sistemático o algo puntual, después se reúnen con la víctima para darle apoyo, ayudarla y tranquilizarla. Hablan también con los acosadores para que sean conscientes de sus acciones y las cambien.

El programa cuenta con materiales de apoyo que se entregan a las escuelas al momento de incluirse a dicho programa, que consta de:

- Manuales para el maestro, lecciones para los alumnos, videos y otros;
- Presentaciones gráficas para las clases, para las reuniones del personal escolar y reuniones con los padres;
- Sitio web para el personal escolar, los alumnos y padres;
- Chalecos de alta visibilidad para las personas que vigilan en los recreos;
- Videojuego y entorno virtual de aprendizaje contra el acoso escolar.

El programa demostró su eficacia de reducción del acoso escolar denunciado por la propia víctima y por sus compañeros, además de disminuir las represalias y aumentar positivamente la apreciación de la escuela, la motivación académica y el rendimiento escolar. KiVA, de acuerdo a estudios, reduce también la ansiedad y la depresión, y tiene un impacto positivo en la percepción de los alumnos del entorno de sus compañeros. El 98%

de las víctimas ha reportado sentir una mejora respecto su caso. Actualmente tiene presencia en el 90% de los colegios finlandeses.

El programa KiVa, por su efectividad, se ha aplicado (o se sigue implementando) en otros países, como: Bélgica, Estados Unidos, Estonia, Francia, Italia, Luxemburgo, Nueva Zelanda, Países Bajos, Reino Unido, Suecia, Sudáfrica, Argentina y ahora también en México.

Dando pasos hacia la Paz. España

Nombre: Dando pasos hacia la Paz.
Objetivo: Prevención de la violencia y mantener un ambiente de paz.
Población objetivo: Estudiantes de nivel primaria y secundaria.
Tiempo de trabajo: Un ciclo escolar.
Metodología:

Este programa español que ha recibido incluso apoyo económico por parte del gobierno vasco, que aunque no trabajó directamente con el cyberbullying, ha ayudado en la disminución de los efectos de éste, debido a la consecución de sus objetivos específicos: potenciar las conductas prosociales y de la empatía, del autoconcepto-autoestima, de la positiva imagen de los demás y de la capacidad para analizar sentimientos, así como un descenso de la ansiedad. Todo a través de la impartición de pláticas para alumnos y maestros divididos en diversos módulos:

- Módulo I: Un proyecto de consenso de valores
- Módulo II: Ante las violencias, el horizonte de los derechos humanos
- Módulo III: Mi grupo y yo por un mundo no violento
- Módulo IV: La transformación de conflictos, una herramienta valiosa
- Módulo V: Estamos con las víctimas;

que apoyados en diversos recursos, herramientas de expresión corporal y actividades en hojas físicas ayudaron en:

- Obtención de una mejora de los adolescentes hacia sí mismos;

- Aumento significativo del rechazo de situaciones de violencia, junto con el aumento de la capacidad empática del individuo, tanto en general como en temas específicos;
- Aumento de la capacidad de comunicación intragrupo;
- Aumento de la inteligencia emocional de los individuos;
- Sensibilización hacia las víctimas de la violencia, junto con la capacidad de analizar esa conducta;
- Fomento de valores prosociales y de respeto por los derechos humanos;
- Aprobación por parte de los adultos sobre las actividades ofrecidas en el programa.

Bibliografía

INEGI. (2017). Módulo sobre ciberacoso 2017: MOCIBA. INEGI. México.

Santoyo Castillo, D., & Frías, S. M. (2014). Acoso escolar en México: actores involucrados y sus características. (C. d. A.C., Ed.) *Revista Latinoamericana de Estudios Educativos (México) , XLIV* (4), 13-41.

Secretaría de Seguridad Pública. (n.d.). *Ciberdelincuencia*. Retrieved 2017 from http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

Televisión, C. R. (Writer). (2017). *Diez formas de prevenir el #Ciberacoso* [Motion Picture]. Andalucía, España.

Actividad académico y tecno-científica sobre ciberseguridad, ciberdelincuencia y protección de los menores. (2016). *El Búho , Edición Especial*.

Avilés, Á.-P. (2013). *X1RED+SEGURA (Por una red más segura)* (Vol. 1). España.

Amigas, P. (n.d.). *CiberBullying*. Retrieved julio de 2017 from Cyberbullying.com: ciberbullying.com

Argensola. (2011). 5. Identidad digital y reputación. *Cuadernos de comunicación evoca , 2*.

Escalae.org. (n.d.). *Programa KiVA anti bullying*. Retrieved 2017 from http://www.escalae.org/programa-kiva-anti-bullying/

Fundación en Movimiento A.C. (n.d.). *Bullyinformate*. Retrieved 2017 from Ponel cara a tu face: http://bullyinformate.org/campanas/ponle-cara-a-tu-face

Fundación en Movimiento A.C. (n.d.). *Fundación en Movimiento*. Retrieved 2017 from http://www.fundacionenmovimiento.org.mx/?gclid=EAIaIQobChMIoZCJzq2s1QIVSU1-Ch0W2QgZEAAYASAAEgIsIfD_BwE

Hernádez Prados, M. Á., & Solano Fernández, I. M. (2007). Cyberbullying, un problema de acoso escolar. *AIESAD, Asociación Iberoamericana de Educación Superior a Distancia , 10*, 17-36.
Garaigordobil, M. (2011). Prevalencia y consecuencias del cyberbullying: una revisión. (U. d. Almería, Ed.) *International Journal of Psychology and Psychological Therapy , 11* (2), 233-254.
Giones-Valls, A., & Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital. (U. d. Barcelona, Ed.) *Textos universitaris de biblioteconomia i documentació , 24*.
INTECO, I. N. (2015). Guía de actuación contra el ciberacoso. Padres y educadores.
KiVA. (n.d.). *KivaProgram*. Retrieved 2017 from Método KiVA en España: http://www.kivaprogram.net/spain
Reyna Ramos, D., & Olivera Gómez, D. A. (2016). Las amenazas cibernéticas . *UNIVERSITA CIENCIA. Revista electrónica de invesitgación de la Universidad de Xalapa* (Especial), 35-55.
red.es. (n.d.). Capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad.