La educación es de todos
Mineducación

CISP
COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI

Protocolo

Prevención del Ciberacoso y delitos en medios digitales

Tabla de contenido

LISTA DE TABLAS

LISTA DE FIGURAS

Agradecimientos

La construcción del “Protocolo para la prevención del Ciberacoso y Delitos en medios digitales” también contó con participación de estudiantes, familias, docentes, directivas de los establecimientos educativos, quienes ejercen la orientación escolar, funcionarias y funcionarios de las secretarías de educación departamentales y municipales, personas expertas de entidades gubernamentales, profesionales de los Ministerios de Salud y Protección Social, de Tecnologías de la Información y las Comunicaciones, representantes de la Policía de Infancia y Adolescencia, del Instituto Colombiano de Bienestar Familiar ICBF, de entidades como UNICEF, RedPapaz, Aulas en Paz, Tigo, Movistar, CISP y académicos-investigadores de España, Suecia, Canadá, Estados Unidos, México y Colombia.

Todas sus experiencias, conocimientos, y sugerencias, fueron determinantes para que este Protocolo se nutriera de la mejor evidencia científica disponible, en aras de constituirse en un insumo orientador de acciones, planes y proyectos para la ciberconvivencia, la prevención y el manejo de riesgos en los entornos digitales en los que interactúan niñas, niños y adolescentes de los establecimientos educativos del país.

Este Protocolo se formuló con los aportes y liderazgo de la experta, investigadora y docente María Clara Cuevas Jaramillo en el marco del convenio suscrito entre el Ministerio de Educación Nacional y el CISP. Se alineó con los demás protocolos que el Ministerio de Educación Nacional ha aportado recientemente, en cumplimiento de su responsabilidad y compromiso con la convivencia de nuestras niñas, niños y adolescentes escolarizados y que señalan acciones para prevenir y abordar las violencias basadas en género, el consumo de sustancias psicoactivas y el suicidio.

Para acceder a los aportes de las personas y entidades antes mencionadas, se efectuaron 12 entrevistas grupales, con estudiantes de grados 5 a 11, familias, docentes y directivos docentes de establecimientos educativos y Escuelas Normales Superiores y profesionales de convivencia escolar de las secretarías de educación representantes de las 5 regiones del país, Atlántica, Andina, Pacífica, Oriental y Amazonía; 4 entrevistas individuales con expertos académicos-investigadores internacionales, y, se recibieron 4 documentos con respuestas a las preguntas orientadoras usadas en las entrevistas, también de 3 expertos académicos-investigadores internacionales. De igual manera, una vez construido el Protocolo, se realizó una validación de lo propuesto, con algunas de las personas participantes del proceso inicial.

Para todas las personas un especial agradecimiento, sus aportes se unieron a los del equipo del Ministerio de Educación Nacional y a investigadores de Canadá, Debra Pepler, Ph. D. de York University y PrevNet; Shelley Hymel. Ph.D. y Jennifer D. Shapka, Ph.D. de University of British Columbia. De Estados Unidos, Pamela Orpinas Ph.D. de University of Georgia, y Ron Slaby Ph.D. del Center on Media and Child Health, Children’s Hospital Boston of Harvard Medical School. De España, Maite Garaigordobil Ph.D. de la Universidad del País Vasco y Rosario Ortega, Ph.D. de la Universidad de Córdoba. De Suecia, Robert Thornberg, PhD. de Linköping University. Y, de México, José Angel Vera, Ph.D. del CIAD- Universidad de Sonora; Marta Vanessa Espejel, Ph.D. y Efraín Duarte, Ph.D. de la Universidad Autónoma de Yucatán. Y a nuestros expertos académicos-investigadores de Colombia, Olga Lucía Hoyos Ph.D. de la Universidad del Norte, Enrique Chaux, Ph.D. de la Universidad de los Andes, Nadia Semenova, Ph.D. y Natalia Cárdenas, Mg. de la Universidad CES, Mauricio Herrera, Ph.D. de la Universidad de Nariño y, Alejandra Vidal, Mg. del Instituto Cisalva de la Universidad del Valle, a quienes también se les agradece su contribución con la educación y la convivencia escolar de Colombia.

A todas y cada una de las personas y entidades, nuestro sincero agradecimiento por sus aportes, y en especial, por su interés genuino en contribuir con ellos al fortalecimiento de la convivencia y ciberconvivencia de nuestros escolares, en el entendido que ello representa un elemento nodal para su formación como seres humanos con la integridad, la ética, las competencias y el compromiso de estas nuevas generaciones.

1. INTRODUCCIÓN

El acoso escolar (AE) en sus diferentes modalidades continúa siendo una preocupación global que amenaza el derecho a la protección contra toda forma de violencia y el derecho a la educación de calidad de niños, niñas, adolescentes y jóvenes (NNAJ). Las cifras dan cuenta de la magnitud del fenómeno, una vez que la UNESCO (2017, 2019) y UNICEF (2018, 2020) reportan que 1 de cada 3 estudiantes (32%) ha sido víctima de AE, y que, 31% de adolescentes informan haber acosado a compañeros. Una manifestación de AE es el ciberacoso, del cual los datos muestran un incremento progresivo en su prevalencia del 5% entre 2010 y 2014, con un estimado global de 12% de niños afectados (Herrera, Romera & Ortega-Ruiz, 2018; Hinduja & Patchin, 2012, 2020; UNESCO, 2019).

En respuesta a los datos, organismos multilaterales y gobiernos, reiteran la importancia de proteger y garantizar los derechos de NNA, incluyendo entre su metas y objetivos el compromiso con su educación de calidad y su protección de la violencia. De manera contundente, la Declaración Universal de los Derechos del Niño (1979), los Objetivos de Desarrollo Sostenible (2015) y el Plan Nacional de Desarrollo de Colombia 2018-2022, enfatizan en tales derechos y en la obligatoriedad de ser garantes de estos. Acorde a ello, el Ministerio de Educación Nacional (MEN), a través de la Ley 1620 de 2013, "Por la cual se crea el sistema nacional de convivencia Escolar y formación para el ejercicio de los derechos Humanos, la educación para la sexualidad y la prevención y Mitigación de la violencia escolar", viene desarrollando estrategias que materializan dicha ley, a través de las cuales el Estado enmarca algunas de sus acciones protectoras, estableciendo mecanismos y acciones que fortalezcan la convivencia escolar, condición ineludible para la calidad de la educación, y la protección de algunas formas de violencia contra NNAJ. El Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y la Mitigación de la Violencia Escolar creado a partir de dicha Ley, es el articulador de acciones de cara a la prevención y atención de las diversas situaciones relacionadas con la convivencia, con las que se vulneran los derechos y se compromete el potencial desarrollo óptimo e integral de los NNAJ. Como parte de la potenciación de dicho sistema, y cumpliendo con el compromiso estipulado por la Ley misma, el MEN trabaja para fortalecer y complementar herramientas existentes a fin de que, en la escuela, entorno privilegiado para la construcción de convivencia y ciudadanía, se cuente con más estrategias pedagógicas para que se prevengan, resuelvan y mitiguen la mayor parte de acciones que amenazan la convivencia escolar. Por ello, se ha dado prioridad a elaboración de nuevos protocolos, con énfasis en las situaciones que, según evidencia actualizada disponible, son las que mayormente afectan el desarrollo integral de los estudiantes.

Para tal propósito, se ha generado una alianza con el Comitato Internazionale Per Lo Sviluppo Dei Popoli (CISP), buscando unir esfuerzos, experiencias, recursos técnicos, programáticos, administrativos y financieros, para que el sector educativo nutra la implementación de estrategias pedagógicas y de movilización social que fortalezcan la convivencia escolar. A través del Convenio de Asociación No. CO1.PCCNTR.1630701 de 2020 suscrito entre el Ministerio de Educación Nacional y el CISP, se establecieron 4 componentes a desarrollar, el segundo de ellos referido al ciberacoso y delitos tecnológicos, cuyo propósito es el diseño del protocolo para la prevención del ciberacoso y delitos tecnológicos que afecten el desarrollo integral de los niños, niñas y adolescentes.

El presente documento contiene el Protocolo para la prevención, atención y mitigación de las situaciones de ciberacoso y delitos tecnológicos que se puedan presentar en la cotidianidad escolar o a partir de las relaciones escolares. El protocolo está enmarcado de manera transversal, por el enfoque de Derechos Humanos, Sexuales y Reproductivos, de género y diferencial -inclusión e interculturalidad- y de justicia restaurativa, que, entre otros, constituyen los enfoques de la Ruta de Atención Integral de Convivencia Escolar promulgada en el 2013, que da origen a la formulación del protocolo.

Tiene como características adicionales la adopción del ciber acoso y delitos tecnológicos no solo como comportamientos problemáticos entre algunos estudiantes, sino como un fenómeno social con particulares dinámicas relacionales que lo sustentan, las cuales han de ser reconocidas e intervenidas (Bacchini, Esposito & Affuso, 2009; Craig & Pepler, 2007; Espelage, 2014; Ettekal, Kochenderfer-Ladd & Ladd, 2015; Lanzillotti y Korman, 2020; Migliaccio y Raskauskas, 2015; Salmivalli, 2010). De igual manera se aborda desde la perspectiva socio ecológica que, en consonancia con lo anterior, proporciona la comprensión de las interacciones entre los numerosos contextos socio ecológicos, escolares, familiares, comunitarios, sociales y culturales, entre otros, que directa o indirectamente aportan al fenómeno (Bronfenbrenner, 1979; Espelage, 2014; Orpinas y Horne, 2006). Se adopta también un abordaje transteórico en el que se vinculan teorías e investigaciones actuales sobre factores que inciden en procesos de cambio personales y colectivos, así como los momentos que están involucrados en tales procesos, retomando lineamientos de cara a facilitar cambios en competencias digitales y socioemocionales, en los grupos de la comunidad escolar (Prochaska y DiClemente, 1982). Vincula además propuestas de diversas disciplinas, que explican el fenómeno de manera más comprensiva, incluyendo visiones del mismo que dan cuenta de factores personales, familiares, escolares, sociales y culturales que contribuyen con su aparición y mantenimiento (Craig & Pepler, 2007; Espelage, 2014; Li, 2007; Machimbarrena, González-Cabrera & Garaigordobil, 2019; Migliaccio y Raskauskas, 2015; Olweus, 2012) y a la vez, arrojan luces para la construcción de las prácticas de prevención y promoción educativas, la definición de rutas de atención cuando las situaciones se presenten o se identifiquen desde el entorno escolar y las rutas para la mitigación de los daños causados tanto a las personas agredidas, como a los agresores y los observadores. Esto último teniendo en cuenta la perspectiva restaurativa que propone el manejo de las situaciones que alteran la convivencia escolar propia de la Ley 1620 de 2013.

Igualmente, la propuesta adopta una mirada de “Escuela Entera” (Craig & Pepler, 2007; Espelage, 2014; Garaigordobil & Oñederra, 2010; Olweus, 2012) en la que todos los actores de la comunidad escolar, directivos, administrativos, familias, docentes y estudiantes participan en su construcción y así mismo son tenidos en cuenta en los lineamientos y acciones que se proponen. Además, focaliza las acciones propuestas en la promoción del bienestar integral -salud mental- y, por ende, promoción del desarrollo integral óptimo de los NNAJ. De otra parte, enfatiza en la formación y fortalecimiento de competencias a través de las cuales, los conceptos, ideas, valoraciones que se aborden sean llevados a la vida y las interacciones escolares cotidianas.

Se apoya además en metas para la educación global particularmente referidas a la educación digital, adoptando el concepto de Inteligencia Digital -DQ- (DQ Institute, 2020) como guía para determinar las competencias socioemocionales y digitales que permiten a los escolares beneficiarse de las oportunidades del ciberespacio para ampliar su aprendizaje, sus relaciones

interpersonales, conectarse con el mundo, disfrutar de diversión en línea, crear y contar con mejores herramientas para su vida y su desarrollo laboral posterior, competencias que a la vez los fortalecen para hacer frente a las amenazas digitales entre las que se encuentra el ciberacoso escolar (Carta de derechos Humanos y Principios para Internet, 2015; Child on line Safety Index Report 2020; Decálogo de E-derechos, Unicef 2004; DQ Global Standars Report 2018, 2020; ODS, 2015; OECD 2030).

Toma también en cuenta los Estándares Globales de Inteligencia Digital, consensuados por las agencias, gobiernos, entidades y universidades que conforman el Movimiento por la Inteligencia Digital, evaluados a través del COSI, Child on line Safety Index, que en 2020 realizó su medición más reciente, con la participación de 30 países, entre ellos Colombia, cuyas puntuaciones la ubicaron en el lugar 20, evidenciando sus áreas fuertes, legislación y normativa de soporte, guía parental a los escolares y, acciones del sector educativo, y, como principales áreas a fortalecer, la exposición a contenidos y contactos de riesgo de los escolares colombianos (DQ Global Standars Report 2020).

Para la construcción del protocolo se implementaron técnicas de investigación cualitativas enmarcadas en el paradigma de la fenomenología y desde una postura socio-crítica que permitieron la gestión del conocimiento recogido de manera coherente y contextualizada, tanto en tiempo como en espacio. Dicho conocimiento implica entonces información referida a prácticas y acciones, decantando de ellas su sentido, para construir con ello las orientaciones que se incluyeron en el protocolo (Carvajal, 2010; Martínez, 2008).

Desde esta perspectiva se realizaron 12 entrevistas grupales y 4 individuales que permitieron estudiar la realidad del ciber acoso y los delitos tecnológicos, desde el contexto natural y las formas en que ocurren, vinculando su comprensión a la perspectiva de propios actores quienes aportaron sus experiencias y sus significados del fenómeno.

Así mismo, se complementó la información con entrevistas a investigadores alrededor del tema, del orden nacional e internacional, y se realizó revisión documental sobre acciones pedagógicas a la vez que se conocieron avances logrados por las Entidades Territoriales y las Instituciones Educativas nacionales, todo esto con el fin de identificar buenas prácticas con posibilidad de ser replicadas en el contexto nacional.

Este protocolo fue sometido a proceso de validación con participantes de todas las zonas socioculturales del país y también por aliados expertos e investigadores nacionales.

Propósito

2. PROPÓSITO

El ciberacoso escolar y los delitos tecnológicos se han convertido en las “nuevas formas” de realizar agresiones entre pares, notándose un incremento dramático en su prevalencia durante los últimos años de 5% entre 2010 y 2014, con un estimado global de 12% de niños afectados (Herrera, Romera & Ortega-Ruiz, 2018; Hinduja & Patchin, 2012, 2020; Ortega-Ruiz, 2020; UNESCO, 2019). El aumento en su incidencia está claramente relacionado con la disponibilidad y el acceso a dispositivos y medios tecnológicos para la comunicación, que cobran especial relevancia para los escolares considerados como la generación digital, quienes los utilizan permanentemente como estrategia relacional preferencial.

Esta socialización digital, si bien conlleva invaluables oportunidades y retos para los escolares, no está exenta de riesgos que pueden amenazar su integridad y su curso óptimo de desarrollo. Uno de estos riesgos es el denominado ciberacoso escolar, también conocido como ciberbullying, o agresión en línea, definido como un comportamiento en línea, agresivo, repetido e intencional, dirigido a una víctima que no puede defenderse fácilmente (Smith et al., 2008). La definición de la conducta de ciberacoso es derivada de la del acoso cara a cara, y en ella se ponen de relieve tres componentes básicos: intencionalidad, repetición y desbalance de poder, que son las condiciones para considerar como acoso una conducta de agresión entre pares escolares. La intencionalidad en ciberacoso es relativamente clara, humillar, degradar, ofender, molestar, burlarse, intimidar o excluir. No obstante, es importante resaltar que, para el acoso en línea, la repetición está dada por el número incontable de veces en que puede ser visto un mensaje o una imagen difundidos a través del internet o de las redes, hecho que victimiza ese mismo número de veces al escolar agredido. Es decir, no se requiere que el agresor repita en otra ocasión la ciberagresión para ser considerada como tal (D. Pepler, comunicación personal, 11, 01, 2020).

En cuanto a la condición de desbalance, se considera que está dada, por la indefensión del agredido frente a su victimización en línea, generalmente su desconocimiento del agresor posiblemente amparado por la condición de anonimato, y su imposibilidad de detener la circulación de la información en su contra, que además puede ocurrir más allá del espacio físico escolar cotidiano, y durante todas las horas y días de la semana. El ciberacoso puede darse a través de diferentes formas, como puede verse en la Tabla 1. consignada a continuación. De gran importancia resaltar que, si bien estas formas de ciberacoso han sido reconocidas en el contexto global, clasificándolas como acciones a través de las cuales se realizan acosos digitales, algunas de las aquí incluidas son consideradas conductas delictivas según la legislación nacional vigente.

Tabla 1. Modalidades del ciberacoso escolar. Adaptado de Flores, 2008; Garaigordobil, 2011 Hinduja & Patchin, 2020; Limber y Agatston, 2010.

Modalidades Ciberacoso Escolar	
Insultos Electrónicos	Comunicación agresiva por medio de las TICS entre dos o más estudiantes, en la que hay intercambio de mensajes a nivel público como privado.
Hostigamiento	Intimidación constante a una o un estudiante determinado, a nivel público y privado, que involucra el envío de varios mensajes de texto en simultánea. Esta agresión es realizada a largo plazo, por uno o más acosadores.
Denigración	Difusión de información denigrante y sin fundamentos sobre otra-o estudiante, enviada a través de páginas web, redes sociales, mensajes de texto u otros; pueden ser fotos alteradas digitalmente, con las cuales pone a esta persona en posición socialmente incómoda y hasta humillante.
Suplantación	Hacerse pasar por otra persona; el agresor accede a las cuentas personales del agredido y desde ahí envía mensajes ofensivos a otras personas, como si hubieran sido enviados por la persona agredida, haciéndola quedar mal con sus amigos.
Desvelamiento y Sonsacamiento	Revelación a cualquier otra persona, de información privada y comprometedora que ha sido sonsacada o hurtada a la persona agredida.
Exclusión	Dejar a un lado a la persona agredida, privándola de la participación en alguna red social, chat o grupo.

Cabe además precisar que, el ciberacoso es la denominación otorgada a la acción agresiva a través de las TIC, pero que su comprensión y abordaje, obligan a una mirada de éste como un fenómeno social producto de dinámicas complejas en las relaciones entre pares escolares, que deben ser reconocidas e intervenidas a fin de reducir su incidencia (D. Pepler, comunicación personal, 11, 01, 2020; Migliacccio y Raskauskas, 2015; R. Thornberg, comunicación personal, 10, 12, 2020; Salmivalli, 2010; Thornberg, 2015; Thornberg, Wänström & Hymel, 2019). Las dinámicas incluyen la adopción de tres roles diferenciales asumidos por los estudiantes, agresores, agredidos y observadores -audiencia-, que pueden ser transitorios o rotativos, los cuales están íntimamente relacionados con el mantenimiento del fenómeno, haciendo del ciberacoso una estrategia relacional “normalizada” por una gran parte de ellos.

Guardan además relación con el momento de curso de vida, particularmente de estudiantes transitando entre grados 6 a 10, para quienes la construcción de la identidad social con los pares y la pertenencia a los grupos se constituye en una tarea del desarrollo y una meta con alto valor motivacional. Por ello, ser “popular”, notarse, tener liderazgo, poder en los grupos, son factores movilizadores que permean sus relaciones y que facilitan adopción de comportamientos que otorgan visibilidad, aún a costa de agredir a otros. No obstante, el papel desempeñado por el grupo (que no es el agresor directo) es decisivo, una vez que otorga visibilidad al agresor, asumiéndolo además como modelo a seguir para alcanzar dicho logro, con lo cual el grupo va validando, normalizando e incluso normatizando este tipo de relaciones agresivas y abusivas,

que llegan a ser asumidas como “normales”, despojándolas de la perspectiva dada por el adulto, de relaciones atentatorias de la convivencia escolar (Cuevas & Marmolejo, 2016; Marwick & Boyd, 2011; Vandebosch & van Cleemput, 2009).

De igual manera la normalización de estas interacciones agresivas recibe influencias de otros contextos relacionales de estudiantes, familiares, institucionales, barriales, culturales, de los medios, entre otros, por lo cual el abordaje del fenómeno implica una visión de la escuela entera, con la participación de todos los miembros de la comunidad educativa, Directivos, Docentes, Familias y Estudiantes mismos, a fin de hacerlos corresponsables del fenómeno y copartícipes de las acciones para su prevención y atención. Adicionalmente, implica acciones pedagógicas concretas que dicha comunidad educativa requiere, de cara a la reducción del fenómeno y al fomento del clima escolar de calidad para todos los educandos.

El ciberacoso escolar está produciendo efectos indeseables en los adolescentes y jóvenes. Se han documentado especialmente para las víctimas, efectos como el aislamiento, la tristeza, la desmotivación, el estrés, pérdida o disminución de autoestima; efectos emocionales y afectivos más severos en la salud mental y el bienestar como ansiedad, depresión, estrés agudo y postraumático, ideación, intentos y comisión de suicidios, y las autolesiones corporales; efectos sociales, con un marcado deterioro en las relaciones entre los compañeros escolares, aislamiento social, exclusión; efectos escolares, referidos a ausentismo, baja pertenencia a la escuela, baja motivación con lo escolar, clima escolar pobre y bajas en rendimiento académico; cognitivos, como dificultades en concentración y atención, menor retención y comprensión, entre otros, que a todas luces evidencian que el fenómeno impacta negativamente el desarrollo integral de los estudiantes tanto que, es considerado un problema de salud mental global (Cowie, 2013; Cross, Lester & Barnes, 2015; D. Pepler, comunicación personal, 11, 01, 2020; Garaigordobil & Oñederra, 2010; Consejería de Educación Junta de Andalucía, 2017; Smith, et al., 2008) y que definitivamente atenta contra su derecho a la protección de la integridad y a la educación de calidad.

Los efectos también incluyen a los agresores, en quienes se ha encontrado mayor probabilidad de adoptar otras conductas de riesgo como el uso temprano y abuso de sustancias psicoactivas y alcohol, relaciones sexuales temprano y sin protección; la adopción de formas agresivas y violentas en los distintos tipos de relaciones que establezcan; la tendencia a obtener metas sociales a través del dominio y la agresión; la posible vinculación con grupos de pares agresivos e incluso delictivos, y la probable comisión de conductas de tipo antisocial y delictivo, es decir, parece darse en este grupo una continuidad en el tiempo de validación y uso de la agresión y la violencia (Farrington & Ttofi, 2011; Ttofi, Farrington & Lösel, 2012; Valdebenito, Ttofi, & Eisner, 2015).

También se han reconocido efectos no deseables para los observadores o audiencia, como la insensibilización ante el sufrimiento del par agredido y de personas victimizadas por acciones agresivas o violentas; la tolerancia frente al uso de la violencia; la adopción de actitudes pasivas ante la injusticia; la normalización de lo violento, que los pone en riesgos similares a los de sus pares agresores. Y, en caso de que los observadores estén en desacuerdo con las ciberagresiones realizadas por sus pares, sin realizar acciones para detenerlas, se han observado efectos emocionales sobre todo relacionados con la ansiedad producida por el temor a ser agredidos en el futuro y además, culpabilizaciones por no actuar para detener las agresiones (Consejería de Educación Junta de Andalucía, 2017; Cuevas y Marmolejo, 2014).

El protocolo para la Prevención del ciberacoso escolar y los delitos tecnológicos va entonces orientado a que los NNAJ se involucren menos en situaciones de riesgo o agresión en línea, promoviendo en ellas y ellos la generación de una sana ciberconvivencia que les permita disfrutar de todos los avances tecnológicos, a la vez que se protegen de ser partícipes o víctimas de acciones que la amenazan, como el ciberacoso, los delitos tecnológicos y otras situaciones riesgosas en línea, ayudándoles a crear y fortalecer su ciudadanía digital, que implica conocimientos, competencias socioemocionales y digitales, valores y actitudes para desenvolverse en la comunidad virtual de manera responsable, segura y ética, usando la tecnología para aprender, crear, divertirse y comunicarse (DQ Institute, 2017).

Pretende por tanto proporcionarles herramientas concretas útiles para dicha ciudadanía y ciberconvivencia, y para la detección y manejo (acorde con la Ruta de Atención Integral para la Convivencia) de las situaciones de vulneración en línea de sus derechos. Involucra, además, lineamientos para acciones pedagógicas con todo el ecosistema protector, a fin de que este opere para educarlos, protegerlos, acompañarlos y fortalecerlos en la construcción de su ciudadanía digital y, en el manejo de situaciones riesgosas o agresiones en línea en las que han participado o han sido victimizados, así como en las acciones de reparación y restauración a las que haya lugar como parte de los procesos.

Es un insumo para que todas las instituciones educativas del país cuenten con conceptos unificados, pautas y lineamientos pedagógicos, específicos para cada miembro de la comunidad educativa, pretendiendo que las acciones sistémicas, coordinadas, conjuntas, adecuadas a las necesidades concretas y a los recursos disponibles sean adaptadas a cada EE, para lograr tal objetivo. Se busca la generación de cambios en todas las instancias comprometidas, que implican instauración y fortalecimiento de competencias de diversa índole, cognitivas, emocionales, comunicativas e integradoras (Chaux, 2012), de cara a que hagan vida cotidiana en las interacciones en línea de los miembros de cada comunidad educativa.

Figura 1. Proceso y participantes Protocolo Ciberacoso y delitos tecnológicos.

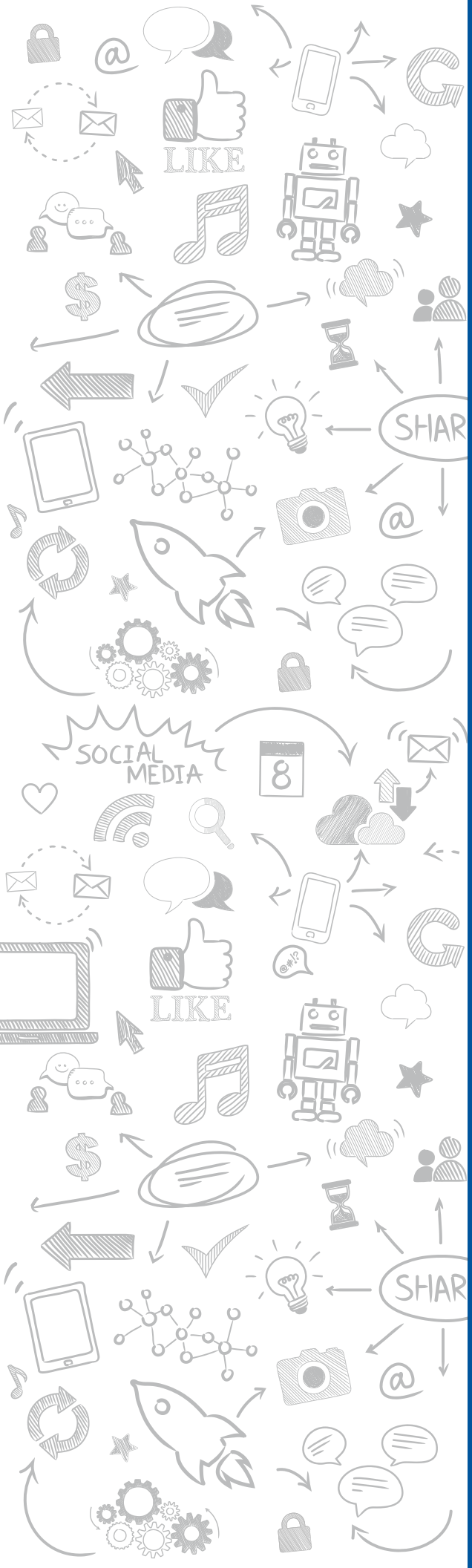
Fuente: Construcción propia

El presente documento contiene el Protocolo para la prevención, atención y mitigación de las situaciones de ciberacoso y delitos tecnológicos que se puedan presentar en la cotidianidad escolar o a partir de las relaciones escolares. El protocolo está enmarcado de manera transversal, por el enfoque de Derechos Humanos, Sexuales y Reproductivos, de género y diferencial -inclusión e interculturalidad- y de justicia restaurativa, que, entre otros, constituyen los enfoques de la Ruta de Atención Integral de Convivencia Escolar promulgada en el 2013, que da origen a la formulación del protocolo.

Tiene como características adicionales la adopción del ciber acoso y delitos tecnológicos no solo como comportamientos problemáticos entre algunos estudiantes, sino como un fenómeno social con particulares dinámicas relacionales que lo sustentan, las cuales han de ser reconocidas e intervenidas (Bacchini, Esposito & Affuso, 2009; Craig & Pepler, 2007; Espelage, 2014; Ettekal, Kochenderfer-Ladd & Ladd, 2015; Lanzillotti y Korman, 2020; Migliaccio y Raskauskas, 2015; Salmivalli, 2010). De igual manera se aborda desde la perspectiva socio ecológica que, en consonancia con lo anterior, proporciona la comprensión de las interacciones entre los numerosos contextos socio ecológicos, escolares, familiares, comunitarios, sociales y culturales, entre otros, que directa o indirectamente aportan al fenómeno (Bronfenbrenner, 1979; Espelage, 2014; Orpinas y Horne, 2006). Se adopta también un abordaje transteórico en el que se vinculan teorías e investigaciones actuales sobre factores que inciden en procesos de cambio personales y colectivos, así como los momentos que están involucrados en tales procesos, retomando lineamientos de cara a facilitar cambios en competencias digitales y socioemocionales, en los grupos de la comunidad escolar (Prochaska y DiClemente, 1982). Vincula además propuestas de diversas disciplinas, que explican el fenómeno de manera más comprensiva, incluyendo visiones del mismo que dan cuenta de factores personales, familiares, escolares, sociales y culturales que contribuyen con su aparición y mantenimiento (Craig & Pepler, 2007; Espelage, 2014; Li, 2007; Machimbarrena, González-Cabrera & Garaigordobil, 2019; Migliaccio y Raskauskas, 2015; Olweus, 2012) y a la vez, arrojan luces para la construcción de las prácticas de prevención y promoción educativas, la definición de rutas de atención cuando las situaciones se presenten o se identifiquen desde el entorno escolar y las rutas para la mitigación de los daños causados tanto a las personas agredidas, como a los agresores y los observadores. Esto último teniendo en cuenta la perspectiva restaurativa que propone el manejo de las situaciones que alteran la convivencia escolar propia de la Ley 1620 de 2013.

Igualmente, la propuesta adopta una mirada de “Escuela Entera” (Craig & Pepler, 2007; Espelage, 2014; Garaigordobil & Oñederra, 2010; Olweus, 2012) en la que todos los actores de la comunidad escolar, directivos, administrativos, familias, docentes y estudiantes participan en su construcción y así mismo son tenidos en cuenta en los lineamientos y acciones que se proponen. Además, focaliza las acciones propuestas en la promoción del bienestar integral -salud mental- y, por ende, promoción del desarrollo integral óptimo de los NNAJ. De otra parte, enfatiza en la formación y fortalecimiento de competencias a través de las cuales, los conceptos, ideas, valoraciones que se aborden sean llevados a la vida y las interacciones escolares cotidianas.

Se apoya además en metas para la educación global particularmente referidas a la educación digital, adoptando el concepto de Inteligencia Digital -DQ- (DQ Institute, 2020) como guía para determinar las competencias socioemocionales y digitales que permiten a los escolares beneficiarse de las oportunidades del ciberespacio para ampliar su aprendizaje, sus relaciones



Del Componente de Prevención

3. DEL COMPONENTE DE PREVENCIÓN

Dadas las características del ciberacoso y los delitos informáticos, que ocurren en las redes, cuentas y sitios frecuentados por los escolares a los que acceden desde sus propios dispositivos, y la imposibilidad de otros para acceder a ellas sin su consentimiento, posiblemente los adultos nunca lleguen a estar informados al respecto, como lo muestran datos de Juvonen y Gross (2008) según los cuales el 90% de los jóvenes nunca informan a un adulto de haber sufrido ciberacoso pues lo consideran parte de su intimidad (Quesland Anti ciberbullying Task Force, 2018; UNICEF-Gobierno de Buenos Aires, 2017).

Además, es frecuente que cuando ocurren situaciones de acoso, los adultos se enteren cuando ha transcurrido cierto tiempo desde el evento, y los escolares implicados estén sufriendo silenciosamente las consecuencias de estas situaciones e incluso haciendo un manejo inadecuado de ellas. Parte de este ocultamiento es debido al temor de los escolares de que, al informar sobre estos hechos agresores, les sean retirados o retenidos sus dispositivos o prohibidos los accesos al internet. Por otro lado, no es posible impedirles el acceso a estas tecnologías puesto que, en ocasiones, cuando en los hogares hay restricciones al respecto, otros pares facilitan dicho acceso. Tampoco es recomendable perseguir a los jóvenes para saber de su vida digital puesto que buscarán estrategias y contextos para evadir vigilancia adulta y socializar por estos medios (Defensor del Menor en la Comunidad de Madrid, 2011; Kowalski, Limber, & McCord, 2019).

Se reitera que, la opción preferencial y entre otras la que se recomienda por parte de expertos en el tema (COST IS 0801, 2013; D. Pepler, comunicación personal, 11, 01, 2020; Hinduja & Patchin, 2020; Queensland Anti-Ciberbullying Task Force, 2018; R. Slaby, comunicación personal, 09, 21, 2020) es el fortalecimiento de competencias en los escolares para que ellos operen como sus propios agentes gestores de sana ciber convivencia, beneficiarios de las ventajas del mundo digital y protectores para sí mismos y para sus pares, de los riesgos involucrados en el. Agencia que obviamente ha de ser proporcional a la edad y nivel de desarrollo, de manera tal que progresivamente se transite desde la protección, regulación y control por parte de los adultos -control externo-, de su acceso y contenidos digitales, hasta la propia regulación y autocontrol –control interno- de exposición y uso de dichos recursos tecnológicos. Así que el objetivo de este nivel de prevención consiste en propiciar o fortalecer competencias para su ciudadanía digital (DQ Institute, 2019; Instituto Nacional de Tecnologías de la Educación INTECO, 2012; UNICEF, 2019)
Esta capacidad de agencia digital se apuntala de manera definitiva en la agencia moral, entendida como la construcción y uso de principios y estándares morales para orientar las propias acciones hacia y con otros, respetando su dignidad y sus derechos (Bandura, 2016). Agencia que también se construye gradualmente en la medida en que adultos cuidadores modelan y educan de manera consistente en dichos valores y principios, de manera tal que frente a situaciones que los involucran, se cuente con guías orientadoras en la toma de decisiones. Agencia moral que debe permear todas y cada una de las acciones en línea bajo el amparo de la posibilidad de estar en el anonimato, y aun así cuidar de sí mismo y de otros con quienes se interactúa (R. Thornberg, comunicación personal, 10, 12, 2020).

Como se puede deducir, en la construcción de agencia digital hay un rol protagónico del adulto familiar o escolar, que se “desvanece” sin desaparecer, en la medida en que el estudiante avanza

en su curso de vida, construyendo y consolidando sus propias competencias. Con los de menor edad, el adulto ejerce control pleno facilitando acceso a contenidos de tipo lúdico, a la vez que contribuye para la creación de hábitos digitales saludables, regulando el tiempo en pantalla y los contenidos. El adulto proporciona, autoriza y acompaña. Con pre -adolescentes, se hacen reflexiones sobre oportunidades y riesgos; se reconocen y ponderan las consecuencias de las acciones digitales; se ilustra sobre riesgos y amenazas, fortaleciendo estrategias para aprovechar el mundo digital y enfrentar tales riesgos, y, se enfatiza la empatía digital. Con adolescentes se reitera su capacidad de gestión y regulación a la vez que se resalta la importancia de manejar adecuadamente situaciones y riesgos digitales, recurriendo a ayuda en los casos que lo ameriten (Common Sense Media, 2020; COST IS 0801, 2013; Del Barrio, 2013; Hinduja y Patchin, 2020; Shapka & Law, 2013).

Figura 2. Rol del adulto en el proceso de construcción de agencia para la ciudadanía digital.

Fuente: Construcción propia

Ese adulto por tanto requiere competencias para su guía y acompañamiento eficaces a niños, niñas o adolescentes, que a la vez disminuyan la brecha digital generacional existente la cual facilita el encubrimiento del mundo digital propio por parte de los menores (Queesland Anti Ciberbullying Task Force, 2018; Unicef- Gobierno de la Provincia de Buenos Aires, 2017). De esta manera, los adultos cuentan con insumos para ejercer su corresponsabilidad en la construcción de competencias para la ciberconvivencia en el estudiantado, a la vez que aumentan su eficacia personal y como cuidadores (R. Slaby, comunicación personal, 09, 21, 2020).
Basados en dicha perspectiva de agencia y acompañamiento eficaz del adulto, se asume el abordaje propio de la promoción, entendida como un proceso participativo dirigido a toda la comunidad educativa, desde el cual se pretende el fortalecimiento en competencias para crear condiciones que garanticen bienestar y la generación de culturas favorables (OMS, OPS, s.f), en este caso un clima escolar propicio para la construcción de aprendizaje integral de los educandos y para una cultura de convivencia, ciberconvivencia, inclusión y protección de los derechos humanos, sexuales y reproductivos en las instituciones educativas del país (Artículo 30 de la Ley 1620 de 2013 Ministerio de Educación Nacional, 2013).

Imprescindible entonces señalar el tipo de competencias específicas que facilitan la construcción de la agencia requeridas para la ciudadanía digital, diferenciadas como regulación y control del tiempo en pantalla, es decir, balance entre interacciones en línea y fuera de línea; creación de identidad digital, que a través de acciones digitales dé cuenta de la identidad integral; el manejo de huella digital, gestada a través de lo que se hace y publica en línea; manejo de la privacidad, acorde con elementos íntimos y no públicos que se comparten; manejo de la seguridad digital, con las claves, cuentas y datos personales; pensamiento crítico frente a contenidos digitales, diferenciando amenazas y contenidos falsos; afrontamiento y manejo del ciberacoso para evitar involucrarse como agresor o detenerlo al ser ciberagredido, y, la empatía digital, elemento nodal para la comprensión y respeto activo de las emociones propias y de otros que resultan de las interacciones y acciones en línea (Common Sense Media, 2019; DQ Global, 2017; Finkelhor et al., 2020; Hinduja, 2020).

Figura 3. Competencias digitales.

Fuente: DQ Institute (2017).

Los objetivos planteados implican cambios en los diversos miembros de la Comunidad Educativa, cambios en la información que se tiene, en las creencias y actitudes sobre el uso de tecnología, sobre la propia eficacia para hacer vida digital sana y acompañar la de los estudiantes, ventajas del uso y los riesgos posibles; en las competencias para involucrarse con diferentes dispositivos y recursos digitales, en el conocimiento de cómo actuar frente a riesgos y amenazas (D. Pepler, comunicación personal, 11, 01, 2020; M. Garaigordobil, comunicación personal, 09, 23, 2020), entre otros, y es menester no perder de vista que existen formas eficaces para facilitar dichos cambios en las personas, como lo propone el Modelo Transteórico del Cambio de Prochaska y Diclemente (1982), quienes afirman que el cambio es un proceso que no se produce con una sola acción y en un solo momento, sino que transita por diversas etapas que facilitan el resultado final.

Se tiene en cuenta que muchas veces las personas no tienen intención de cambiar, momento inicial, no saben qué deben cambiar, con lo cual, las primeras acciones deberán estar encaminadas a sensibilizar para motivar el cambio de conducta, facilitando información conducente a la reflexión respecto al estado actual y lo que ello conlleva en relación con la meta. Elementos a favor y en contra de permanecer en la situación presente. Desde el EE, actividades dirigidas a toda la comunidad educativa en las que se evidencien ventajas y oportunidades del mundo digital, riesgos, y se deje ver la importancia de construir conjuntamente una ciudadanía digital promotora de la convivencia, a la vez que se informa sobre consecuencias personales, grupales e institucionales del uso inadecuado de la tecnología digital.

Otro momento importante en los procesos de cambio, se refiere a la adopción de una intención clara de cambio, considerando los pros y contras sobre la vida y las condiciones actuales, claridad respecto a las acciones requeridas para el logro de las metas, a las implicaciones de esa corresponsabilidad de cuidado personal y mutuo en el mundo digital. Dicho análisis favorece hacer el balance de posibles pérdidas y ganancias asociadas a los cambios desde cada individuo, con lo cual la decisión es personal, propia y real. Las acciones y actividades institucionales en esta dirección han de propiciar espacios en los que la comunidad educativa, tenga oportunidad de realizar estos procesos reflexivos, en los que adicionalmente se evidencien brechas a subsanar desde las instituciones mismas.

Como momento posterior se da la preparación desde la que se avanza hacia el logro de la meta, mediante el fortalecimiento o adquisición de las competencias requeridas y la organización contextual que dé apoyo a los cambios proyectados, planificando así las estrategias a adoptar. El EE, tras los balances realizados en momentos anteriores, determina con la comunidad educativa, el proceso pertinente, el plan institucional de fortalecimiento de competencias digitales y socioemocionales para lograrlo, insertándolo al PEI en relación con la convivencia. Para ello, se proyectan acciones diferenciales, acordes con las competencias y necesidades de cada grupo de la comunidad educativa, en términos de las mencionadas competencias digitales y socioemocionales requeridas.

Una vez determinado el plan, se procede con su ejecución, teniendo claro que en cada paso avanzado, se consolidan y fortalecen competencias y condiciones para el siguiente, lo cual se refleja claramente en el proceso de formación y acompañamiento gradual, acorde además con los momentos de curso de vida de los estudiantes, particularmente con sus desarrollos cognitivos y socio-emocionales, que entre otras determinan sus motivaciones y usos de la tecnología digital y, en ese orden de ideas, permiten focalizar las acciones necesarias con el ciber entorno protector, para que cumpla su función de manera eficaz.

Finalmente, el mantenimiento del cambio estará soportado por transformaciones en las condiciones personales e institucionales mencionadas, que requieren permanencia en el tiempo, de manera tal que se constituyan en elementos del contexto cotidiano. Los EE mantendrán acciones, proyectos y programas, harán seguimiento a sus efectos, de cara a que los cambios sean el clima proyectado en el que la ciberconvivencia sea parte de las formas relacionales institucionales en las que se trabaja cotidianamente. Así pues, las pautas contenidas en este protocolo incluyen propuestas que aborden los elementos comprendidos en los procesos de cambio, pretendiendo que haya efectos visibles y concretos que se traduzcan en una contribución a la convivencia escolar.

Figura 4. Las etapas den el proceso de cambio.

Adaptado de Prochaska y DiClemente (1982).

3.1 Promoción de la ciberconvivencia.

Apalancadas en los referentes anteriores, las acciones pedagógicas que se proponen están diferenciadas para cada miembro de la comunidad escolar, es decir, directivos, docentes, Comité de Convivencia, estudiantes y familias, entendiendo que el logro de efectos evidentes será posible en la medida en que las acciones sean realizadas de manera planeada, coordinada, con permanencia en el tiempo. El resultado final pretendido será una información de base generalizada, sobre la tecnología digital disponible y, además, válida y confiable, procedente de fuentes autorizadas, sobre los riesgos y sus consecuencias. Así mismo, se persigue fortalecer competencias técnicas (digitales) y socio-emocionales para los usos adecuados de la tecnología por parte de la comunidad escolar.

Nótese en la Figura 3 sobre componentes de acción para la ciberconvivencia a continuación, la proporción mayor de la promoción, asumiendo que, se han de realizar acciones variadas para el fortalecimiento de competencias las cuales operan como protectores contra los riesgos y ciberamenazas digitales, con lo cual se pretende que las atenciones a situaciones que la afectan sean cada vez menores.

Figura 5. Acciones para la ciberconvivencia y prevención ciberacoso y delitos tecnológicos.

Fuente: elaboración propia.

3.1.1. Acciones pedagógicas de promoción para Directivos Institucionales y Comité Escolar de Convivencia.

Los Directivos tienen un rol preponderante en la generación de una cibercultura institucional adecuada en sus EE puesto que ellos como cabeza visible de la organización marcarán las pautas institucionales, facilitarán condiciones y apoyarán las acciones y programas.

Para ellos se recomienda,

a. Tener información básica actualizada sobre recursos tecnológicos, condiciones de accesibilidad y conectividad, y usos.
b. Realizar "inventario" de recursos y necesidades institucionales en dotación, usos, capacidad docente, familiar y estudiantil para el uso de recursos digitales y la creación de ciberconvivencia.
c. Facilitar la dotación de equipos, dispositivos y plataformas tecnológicas para uso institucional.
d. Propender por mejoras en conectividad y generación de espacios con los dispositivos institucionales para usos académicos y recreativos de estudiantes, a fin de reducir barreras de acceso digitales.
e. Propiciar evaluaciones institucionales de riesgos y protectores de la ciberconvivencia, lectura de contexto, con miras a ajustar las acciones planeadas de manera que sean responsivas a dichos resultados.

f. Conformar un "grupo tecnológico líder" para promover, acompañar y monitorear el uso de equipos y plataformas tecnológicas como recursos pedagógicos a incluir en las asignaturas y las actividades escolares.
g. Promover y verificar que los planes, acciones y programas para la promoción de la ciberconvivencia y uso adecuado de recursos digitales, estén apoyados y nutridos desde y por las acciones institucionales transversales – proyectos pedagógicos - para el fortalecimiento de la convivencia escolar.
h. Gestionar con el Comité de Convivencia la planeación y el apoyo a espacios informativos y formativos sobre recursos y competencias digitales para la comunidad escolar.
i. Construir un directorio de "aliados estratégicos expertos" externos a la institución, que puedan ofrecer capacitaciones y asistencia técnica sobre usos adecuados de la tecnología, para apoyar las acciones institucionales.
j. Gestionar capacitaciones para la comunidad educativa con dichos aliados u otros entes capacitados para tal propósito.
k. Facilitar tiempo al personal docente y de apoyo, para su formación y actualización en el uso de recursos tecnológicos.
l. Proveer espacios curriculares constantes para el fortalecimiento de la ciberconvivencia con los estudiantes.
m. Propiciar incentivos para el desarrollo de campañas, preferiblemente realizadas a través de recursos tecnológicos, para la sensibilización sobre los usos adecuados de la tecnología y la construcción de la ciberconvivencia.
n. Vincular a las familias en la planeación y realización de acciones institucionales para la promoción de la ciberconvivencia y el uso adecuado de los recursos tecnológicos.
o. Otorgar protagonismo a los estudiantes, ciudadanos digitales, en la planeación y realización de acciones institucionales para la promoción de la ciberconvivencia y el uso adecuado de los recursos tecnológicos.
p. Instaurar reconocimiento institucional de acciones de ciberconvivencia por parte de los estudiantes.

3.1.2. Acciones pedagógicas de promoción para Docentes y Orientadores

En la construcción de la convivencia en general y la ciberconvivencia en particular, el rol docente es fundamental, puesto de funge como modelo, figura de apoyo, guía, y líder de la convivencia en el aula. A la vez, es el vigía del cumplimiento de las políticas y acuerdos institucionales sobre la convivencia, adecuándolos en todo caso a las condiciones propias de cada grupo, y es el nexo comunicativo con el ecosistema protector de los estudiantes (Cross, et al., 2016). Para el ejercicio pleno de dichos roles es menester que cuente con información y competencias específicas, que entre otras están orientadas a su interacción con el establecimiento educativo, las familias, los estudiantes y sus colegas (COST IS 0801, 2013; Gradinger, Yanagida, Strohmeier & Spiel, 2016; Queensland Anti Ciberbullying Task Force, 2018).

Para ellos se propone,

3.1.2.1. Para los propios docentes:

a. Revisar y reevaluar creencias y actitudes sobre el uso propio de recursos digitales y su uso por parte de los estudiantes.
b. Complementar su información sobre uso adecuado de recursos digitales.
c. Fortalecer competencias para uso de recursos, dispositivos, plataformas, redes sociales y juegos en línea, preferentemente los más usados por sus estudiantes, a fin de reducir la brecha generacional digital.
d. Involucrarse en la construcción y revisión de políticas, acuerdos, acciones y planes institucionales para el fomento de buen uso de recursos digitales y la construcción de la ciberconvivencia.

3.1.2.2. Con los estudiantes:

a. Fortalecer estrategias comunicativas abiertas, respetuosas y cálidas que faciliten compartir el cibermundo de unos y otros.
b. Construir y fortalecer vínculos cimentados en la confianza mutua, desde la cual puedan expresarse dudas, emociones, expectativas y experiencias asociadas al uso de las tecnologías.
c. Ser modelo del uso adecuado de recursos digitales, con fines pedagógicos, innovadores, lúdicos y comunicativos, cuidando siempre de si mimo y de otros en la red.
d. Incentivar usos adecuados de recursos digitales en las asignaturas y actividades a cargo, estableciendo que los productos solicitados se hagan en formas innovadoras con formatos digitales, tipo video, videoclip, podcast, tutorial, etc.
e. Explorar la información y las competencias de los estudiantes en el uso de tecnología, sus alcances y sus riesgos, mediante análisis de casos, de videos, simulación de situaciones en línea.
f. Tener en cuenta el momento de curso de vida de sus estudiantes en lo que respecta a usos y funciones de dispositivos y tecnología digital, teniendo claro el carácter lúdico para los de menor edad y, el relacional para pre-adolescentes y adolescentes.
g. Planear con los estudiantes acciones y actividades, de aula o institucionales, en las que se resuelvan necesidades informativas de la comunidad educativa sobre uso adecuado, oportunidades y riesgos de los recursos digitales.
h. Establecer metas claras para acompañar a sus estudiantes en la construcción de ciudadanía digital y ciberconvivencia, ayudándoles en la construcción de sus perfiles, apertura de sus cuentas, selección de información a publicar, búsqueda de páginas y portales informativos, académicos, lúdicos y de socialización, acordes también con curso de vida.
i. Identificar en sus grupos, estudiantes digitalmente muy competentes, para vincularlos a las acciones proyectadas de información y formación, para el mismo grupo para estudiantes de grados inferiores.
j. Sensibilizar a estudiantes sobre su responsabilidad con la información digital propia y de otros a la que tengan acceso, resaltando su rol de participantes activos en lo que se publica y se reenvía.
k. Clarificar con estudiantes que el anonimato no exime de responsabilidades para consigo mismos y con otros con quienes interactúa en línea.
l. Fomentar en los estudiantes el uso de sus competencias socio-emocionales y

ciudadanas para sus relaciones en línea.
m. Fortalecer en sus estudiantes el razonamiento moral frente a situaciones que ocurren en la convivencia digital, ayudándoles a considerar su responsabilidad en éstas y el derecho de los agredidos a ser respetados en su integridad e intimidad.
n. Alertar a los estudiantes sobre la permanencia en línea de la información publicada, realizando ejercicios de rastreo de imágenes, noticias y comentarios de épocas remotas.
o. Concertar con los estudiantes la "Netiqueta" o acuerdos de ciberconvivencia, analizando los pros y los contras, para ellos y para los otros, de cada "regla" propuesta, a fin de asegurar la viabilidad de su cumplimiento.
p. Propiciar espacios para que los estudiantes vinculen sus competencias digitales a planes y proyectos institucionales de apoyo a una cultura institucional de convivencia.
q. Fortalecer competencias digitales adecuadas para la ciberconvivencia en estudiantes con condiciones de liderazgo, vinculándolos a grupos de influenciadores y youtubers.

3.1.2.3. Con las familias:

a. Generar espacios de encuentro en los que se reconozcan recursos y necesidades parentales para el acompañamiento de las niñas, niños, adolescentes y jóvenes en la construcción de su ciudadanía digital.
b. Informar a instancias de coordinación y /o Comité Escolar de Convivencia, sobre recursos y necesidades parentales para el acompañamiento de estudiantes en la construcción de su ciudadanía digital, para proyectar acciones institucionales generales.
c. Sensibilizar a las familias en la importancia de realizar acompañamiento a niñas, niños, adolescentes y jóvenes en el uso de recursos y medios digitales, mediante análisis de casos, revisión crítica de videos, etc.
d. Informar a las familias sobre las necesidades diferenciales de acompañamiento a niños, niñas, adolescentes y jóvenes, acordes con su curso de vida, relaciones y usos de los recursos digitales, con control parental sobre acceso a dispositivos, usos y tiempo empleado, con los más pequeños, hasta el apoyo en el manejo de situaciones en línea cuando sea necesario, con los de mayor edad.
e. Concertar y planear acciones colaborativas con las familias para fortalecer la i información y formación sobre uso de recursos digitales.
f. Propiciar encuentros para reconocer, reflexionar y re- evaluar creencias y actitudes sobre el uso de recursos digitales propio y por parte de estudiantes, ajustándolas a fin de no satanizar el uso de los recursos y tener expectativas adecuadas a los usos diferenciales de los recursos de acuerdo con la edad de los niños, niñas, adolescentes y jóvenes.
g. Generar espacios para el fortalecimiento de prácticas de crianza parentales que promuevan la comunicación asertiva niños-familias, en la que se incluya la educación a éstos en el uso adecuado de la tecnología.
h. Alentar a los padres a solicitar información a sus niños, niñas, adolescentes y jóvenes sobre usos de tecnología digital en la que ellos y ellas son expertos.

3.1.3. Acciones pedagógicas de promoción en los estudiantes

Considerando a estudiantes como generación digital, con relativo dominio del uso de recursos digitales, internet y redes sociales, se busca hacerlos protagonistas centrales en la construcción de la ciberconvivencia y su ciudadanía digital, a la vez que apoyan en su ecosistema protector, información y competencias para que los acompañen en este proceso, de manera activa, eficaz y acorde con sus necesidades de ciclo de vida. Se resalta su capacidad de agencia, meta final en este proceso, que debe ser paulatinamente propiciada y acompañada (Defensor del Menor en la Comunidad de Madrid, 2011; Estévez, Flores, Estévez, J. & Huescar, 2019; Hinduja, 2020; Hinduja y Patchin, 2020; M. Garaigordobil, comunicación personal, 09, 23, 2020; P. Orpinas, comunicación personal, 09, 17, 2020; R. Slaby, comunicación personal, 09, 21, 2020; R. Thornberg, comunicación personal, 10, 12, 2020; Queensland Anti Ciberbullying Task Force, 2018; UNICEF, 2017, 2019).

Para ellos se sugiere

a. Revisar sus conocimientos y competencias para el uso adecuado de la tecnología digital y las interacciones en línea.
b. Aclarar sus metas personales en la interacción digital, -instaurar, fortalecer o aumentar relaciones; obtener reconocimiento o notoriedad social o, divertirse-.
c. Explorar sus actitudes y creencias sobre uso de recursos digitales, derechos y responsabilidades, ciberconvivencia, y ciudadanía digital.
d. Analizar pros y contras de construir ciudadanía digital y ciberconvivencia.
e. Reconocer las múltiples opciones de socialización adecuada a través de recursos digitales.
f. Usar sus competencias socio-emocionales y ciudadanas, en la construcción de su ciudadanía digital y su socialización a través de redes.
g. Reconocer su responsabilidad moral con las consecuencias que sus acciones en línea puedan producir sobre otras personas, conocidas o no.
h. Regular su tiempo de uso de pantallas, y su exposición a contenidos y contactos en línea.
i. Conocer políticas y acciones escolares para la ciberconvivencia.
j. Proponer y participar en acciones institucionales para la información y la formación en el uso adecuado de recursos digitales.
k. Reconocer las normas grupales con respecto a la ciberconvivencia.
l. Construir con pares normas de Netiqueta, basadas en acuerdos y determinación de pros y contras.
m. Acordar con pares formas de presión positiva y estrategias concretas para fomentar y mantener la ciberconvivencia.

Nótese que las acciones propuestas tienen en cuenta las etapas de procesos de cambio, pretendiendo que estas se enfoquen en facilitar espacios y actividades en los que la comunidad escolar tenga oportunidades para considerar las posibilidades de cambios personales e institucionales respecto a la ciberconvivencia, a la vez que incluyen análisis de pros y contras relacionados con el posible cambio. De igual manera promueven el fortalecimiento de información y competencias técnicas y socio-emocionales involucradas en la ciberconvivencia escolar, acciones que propician la consolidación de pasos hacia el cambio.

3.2. Prevención de riesgos tecnológicos

Entendiendo la prevención como las acciones encaminadas a evitar o minimizar resultados no deseados en presencia de riesgos, se cuenta con vías distintas para tal objetivo, muchas de las cuales apuntan al fortalecimiento de protectores (Decreto 1965, 2013). Desde este abordaje se hace imprescindible determinar riesgos y protectores, teniendo claro que unos y otros son probabilidades una vez que la evidencia empírica demuestra que estos suelen encontrarse de manera muy frecuente asociados a resultados positivos o negativos en la salud, la convivencia y el bienestar.

Los resultados no deseados en el uso de tecnología digital en escolares están referidos a verse expuestos a las distintas formas de amenazas "on line", entre las que se destacan el uso excesivo de internet, redes y dispositivos; la exposición a contenidos riesgosos, sean estos violentos o sexuales; el establecer contactos de riesgo especialmente con extraños; las ciberamenazas a la seguridad personal en cuentas y perfiles; el ciberacoso y, los riesgos a la reputación personal y la de otros (DQ 2018). En este nivel de intervención escolar entonces, las acciones están encaminadas a promover y fortalecer protectores que, impidan la exposición al riesgo, disminuyan los efectos del riesgo cuando este no se ha podido evitar o, hagan más transitorios y menos severos los efectos de la exposición al riesgo, en términos de Rutter (2000), acciones que propician la resiliencia, a lo cual se adhiere el presente protocolo, asumiendo tales riesgos como oportunidades para el fortalecimiento personal e institucional, más que como situaciones frente a las cuales es inevitable el daño. Esta perspectiva igualmente conlleva a la consideración de la prevención desde un abordaje proactivo que aumenta la eficacia personal e institucional, en lugar de un abordaje desde el temor y la inactividad (Finkelhor et al., 2020).

Siendo el ciberacoso uno de los riesgos en línea a los que más están expuestos los estudiantes (COST IS 080, 2013; DQ Institute, 2020; Unesco, 2019) , afectando claramente la convivencia y la ciberconvivencia, que por ser una forma de acoso escolar ha sido objeto de numerosas investigaciones, se han determinado riesgos y protectores asociados a éste, desde la mirada de Bronfenbrenner (1979) sobre los factores que interactúan en el desarrollo humano, siendo facilitadores o amenazas para dicho desarrollo; a continuación, en la Tabla 2 se señalan tanto riesgos como protectores, individuales, familiares o escolares, que se han reconocido asociados a las condiciones de agresores, agredidos y observadores en situaciones de ciberacoso escolar.

Con respecto a esta ciberamenaza cabe recordar que, los roles no son estáticos ni son características personales de los estudiantes involucrados, puesto que ocasionalmente los agresores pueden llegar a ser agredidos y observadores de agresiones hacia otros, los agredidos pueden tornarse en agresores, sobre todo para hacer retaliaciones por las agresiones recibidas, y, los observadores pueden ser agresores o agredidos.

3.2.1. Factores de riesgo personales para ser agredido en situaciones de ciberacoso

Tabla 2. Riesgos y protectores personales para ser víctima de ciberacoso

SER AGREDIDO - Víctima	
Factores Personales	
RIESGOS	**PROTECTORES**
• Uso diferencial de tecnología (< edad= juegos en línea, >edad= redes sociales). (DePaolis & Williford, 2015; Watts, Wagner, Velasquez, & Behrens, 2017; Whittaker & Kowalski, 2015).	• Alta auto-estima (Álvarez-Garcia et al. (2015)
• Ser víctima de acoso "cara a cara" (Chen, Ho, & Lwin, 2016; Guo, 2016; Kowalski, Giumetti, Schroeder, & Lattanner, 2014; Olweus, 2013).	• Inteligencia social (Kowalski et al., 2014)
• Ser mujer (Shapka, Onditi, Collie, & Lapidot-Lefler, 2018).	• Empatía (Kowalski et al., 2014)
• Ser miembro de comunidad LGBT (Elipe & Del Rey, 2017).	• Auto-eficacia para la propia defensa emocional (Chen et al., 2016).
• Tener sobrepeso (Kenny, Sullivan, Callaghan, Molcho, & Kelly, 2017).	• Auto-regulación emocional (Chen et al., 2016).
• Tener condición de discapacidad o crónica de salud (Beckman, Stenbeck, & Hagquist, 2016).	
• Baja auto-estima (Brewer & Kerslake, 2015; Chen et al., 2016).	
• Poco apoyo de pares (Baldry, Farrington, & Sorrentino, 2016; Fridh, Lindström, & Rosvall, 2015; Kowalski, Giumetti, Schroeder, & Lattanner, 2014).	

3.2.2. Factores de riesgo familiares para ser agredido en situaciones de ciberacoso

De igual manera se reconocen factores familiares asociados a la condición de ser agredido en situaciones de ciberacoso, los cuales se observan en la Tabla 3 a continuación.

SER AGREDIDO - Víctima	
Factores Familiares	
RIESGOS	**PROTECTORES**
• Hogares mono-parentales (Bevilacqua, Shackleton, Hale, Allen, Bond, Christie, Viner, 2017).	• Calidez Parental ((Elsaesser, Russell, Ohannessian, & Patton, 2017).
• Contexto familiar negativo (Guo, 2016).	• Apoyo parental (Martins, Veiga Simão, Freire, Caetano, & Matos, 2016).
• Conflictos familiares (Ortega- Barton, Buelga, & Cava, 2016).	• Relaciones positivas padres-hijos (Fridh et al., 2015).
• Bajo apego parental (Chang, Chiu, Chen, Miao, Lee, Chiang, & Pan, 2015).	• Reglas parentales uso tecnologías (Baldry et al., 2015; Chen et al., 2016; Kowalski et al., 2014)
• Falta de supervisión parental uso de tecnologías (Baldry et al., 2015; Chen et al., 2016; Kowalski et al., 2014)	• Supervisión parental uso de tecnologías (Baldry et al., 2015; Chen et al., 2016; Kowalski et al., 2014)

3.2.3. Factores de riesgo escolares para ser agredido en situaciones de ciberacoso

Así mismo, se identifican factores protectores y de riesgo relacionados con lo escolar, Tabla 4.

Tabla 4. Riesgos y protectores escolares para ser víctima de ciberacoso

SER AGREDIDO - Víctima	
Factores Escolares	
RIESGOS	**PROTECTORES**
• Percepción de inseguridad escolar (Bottino, S., Bottino, C. C., Regina, Correia, & Ribeiro, 2015).	• Satisfacción con la escuela (Lee &Song, 2012).
	• Percepción de seguridad escolar (Kowalski et al., 2014)
	• Clima escolar positivo (Kowalski et al., 2014)
	• Relaciones cercanas con los docentes (Lee, Hong, et al., 2017; Ortega-Barton et al., 2016).
	• Percepción de seguridad escolar (Kowalski et al., 2014)

3.2.4. Factores de riesgo personales para ser agresor en situaciones de ciberacoso

De igual manera se han reconocido los riesgos y protectores asociados a ser agresor en situaciones de ciberacoso escolar, también personales, familiares y escolares.

Tabla 5. Riesgos y protectores personales para ser agresor en situaciones de ciberacoso

SER AGRESOR	
Factores Personales	
RIESGOS	**PROTECTORES**
• Tiempo en línea (Uso diferencial de tecnología < edad= juegos en línea, >edad= redes sociales). (Chen, et al., 2016; Guo, 2016; Kowalski, et al., 2014; Shapka et al., 2018).	• Alta auto-estima (Álvarez-Garcia et al. (2015)
• Ser agresor en situaciones de acoso "cara a cara" (Baldry, Farrington, & Sorrentino, 2016; Kowalski et al., 2014).	• Inteligencia social (Kowalski et al., 2014)
• Desinhibición por el anonimato en línea (Lee, 2017).	• Empatía (Kowalski et al., 2014)
• Haber sido victimizado en acoso "cara a cara" (Souza, Veiga Simao, Ferreira, & Costa Ferreira, 2017).	• Auto-eficacia para la propia defensa emocional (Chen et al., 2016).
• Baja empatía cognitiva y afectiva (Baldry et al., 2015; Brewer & Kerslake, 2015; Del Rey, Lazuras, Casas, Barkoukis, Ortega-Ruiz, & Tsorbatzoudis, 2015; Peterson & Densley (2017).	• Auto-regulación emocional (Chen et al., 2016).
• Baja auto-estima (Baldry et al., 2015; Chen et al., 2016).	
• Desconexión moral (Baldry et al., 2015; Chen et al., 2016; Guo, 2016; Kowalski et al., 2014; Thornberg, Pozzoli, Gini, & Hong, 2017; Thornberg, R., Thornberg, U. B., Alamaa, & Daud, 2016; Thornberg, Wänström, Elmelid, Johansson & Mellander 2020).	
• Creencias favorables al uso agresión (Guo, 2016; Kowalski et al., 2014).	
• Problemas de conducta (Bottino et al., 2015; Guo, 2016).	
• Pertenencia a grupos con problemas de conducta (Lianos & McGrath, 2017).	
• Influencia negativa y presión del grupo de pares (Baldry et al., 2015; Guo, 2016).	
• Necesidad de dominar en el grupo de pares (Watts, Wagner, Velasquez & Behrens, 2017).	

3.2.5. Factores de riesgo familiares para ser agresor en situaciones de ciberacoso

También se destacan los factores familiares protectores o riesgos para la condición de agresores. Tabla 6 a continuación.

Tabla 6. Riesgos y protectores familiares para ser agresor en situaciones de ciberacoso

SER AGRESOR	
Factores Familiares	
RIESGOS	**PROTECTORES**
• Falta de apoyo familiar (Martins, Veiga Simão, Freire, Caetano, & Matos, 2016).	• Calidez Parental (Elsaesser, Russell, Ohannessian, & Patton, 2017).
• Contexto familiar negativo (Guo, 2016).	• Apoyo parental (Martins, Veiga Simão, Freire, Caetano, & Matos, 2016).
• Conflictos familiares (Ortega- Barton, Buelga, & Cava, 2016).	• Relaciones positivas padres-hijos (Fridh et al., 2015).
• Bajo apego parental (Chang, Chiu, Chen, Miao, Lee, Chiang, & Pan, 2015).	• Apoyo emocional familiar Elsaesser et al., 2017; Fanti et al., 2012; Sung, Kim, Lee, & Lim, 2006; Wang et al., 2009).
• Falta de supervisión parental uso de tecnologías (Baldry et al., 2015; Chen et al., 2016; Kowalski et al., 2014)	

3.2.6. Factores de riesgo escolares para ser agresor en situaciones de ciberacoso

Así mismo, se han diferenciado factores escolares relacionados con ser agresor en situaciones de ciberacoso escolar.

Tabla 7. Riesgos y protectores escolares para ser agresor en situaciones de ciberacoso

SER AGRESOR	
Factores Familiares	
RIESGOS	**PROTECTORES**
• Percepción de inseguridad escolar (Bottino, S., Bottino, C. C., Regina, Correia, & Ribeiro, 2015).	• Satisfacción con la escuela (Lee & Song, 2012).
• Falta de reglas escolares claras sobre ciberacoso (Baldry et al., 2015).	• Percepción de seguridad escolar (Kowalski et al., 2014)
	• Clima escolar positivo (Kowalski et al., 2014)
	• Relaciones cercanas con los docentes (Lee, Hong, et al., 2017; Ortega-Barton et al., 2016).

Adaptadas de Kowalski, Limber & McCord (2019).

3.2.7. Riesgos digitales

De cara a la prevención es importante también tener claridad respecto a qué es lo que se considera ciberamenaza a la que pueden verse expuestos los escolares y cómo estas son clasificadas. Se denomina como tal, a todo material electrónico con el cual se puede causar daño o violencia, a sí mismo o a otros, y que puede resultar en violación de DHH o DHSR (Hinduja & Patchin, 2020). Estas ciberamenazas o riesgos digitales se han categorizado como de contacto, de contenido y de conducta.

Las ciberamenazas de contacto se refieren a aquellas situaciones en línea en las que estudiantes participan en comunicaciones e interacciones con personas desconocidas quienes buscan crear contactos inapropiados que de alguna manera ponen en riesgo su salud o bienestar, su seguridad personal, que pretenden fines sexuales, intentan inculcar ideas radicales políticas o religiosas, inducirlos a vinculación a grupos al margen de la ley, a realizar acciones de violencia, odio o discriminación, o, hacerse daño a sí mismos.

Las ciberamenazas de contenido están igualmente referidas a acceder a sitios web con contenidos no deseados o inapropiados que pueden contener pornografía, imágenes violentas, material racista, sexista, xenófobo, homofóbico, de odio, y, aquellos en que se promueven vinculaciones a conductas poco saludables o que engendran riesgos para salud como anorexia, bulimia, exaltación del suicidio. Finalmente, las ciberamenazas de conducta, son aquellos comportamientos digitales en los que estudiantes contribuyen con la producción, reproducción, publicación o distribución, de materiales de riesgo, amenazantes, violentos, o, con contenidos privados, y/o eróticos, que se han producido dentro de relaciones íntimas sin perseguir fines de distribución a otros, y, conductas para realizar ciberacoso a pares escolares (Hinduja, 2020; Hinduja y Patchin, 2020; Instituto Colombiano de Bienestar Familiar, 2019; Livingstone, Haddon, Görzig & Ólafsson, 2011; Unicef, 2017, 2019). En la Tabla 9 puede observarse la categorización de las ciberamenazas.

Tabla 8. Tipos de ciberamenazas

TIPOS DE RIESGOS EN LÍNEA			
Característica	**Contenido**	**Contacto**	**Conducta**
AGRESIVO	Violento, sangriento	Acoso, acecho	Ciberacoso, actividad hostil hacia pares
SEXUAL	Pornográfico	Grooming, abuso o explotación sexual	Acoso sexual y sexting
VALORES	Odio, racismo, sexismo	Persuación Ideológica, adoctrinamiento	Contenido potencialmente dañino generado por el usuario
COMERCIAL	Fines comerciales y de mercadeo	Uso de información personal	Infracciones, derechos de autor, robo de datos

3.2.8. Señales de alerta ser agredido o agredir digitalmente

Finalmente, como insumo adicional que aporta a la prevención y la detección temprana se han reconocido y agrupado señales en escolares que pueden ser asociadas a estar siendo agredido en línea o, estar actuando como ciberagresor (Hinduja y Patchin, 2019; Mueller, 2012) y, que facilitan a los adultos o pares que las reconocen prestar atención a su continuidad e indagar sobre posibles causas, siendo el cieberacoso una de ellas. Dicho reconocimiento temprano favorece que posterior a verificaciones pertinentes, se opte rápidamente por medidas que ayuden a minimizar el efecto negativo del ciberacoso en escolares involucrados. Muy importante destacar que dichas señales deben haber aparecido súbitamente y no deben ser las formas habituales de comportamiento en dichos escolares. En la Tabla 9 a continuación se observan las señales de alerta de ser cibergredido o estar ciberagrediendo.

Tabla 9. Alertas tempranas estudiantes ciberagredidos o cibergresores.

SEÑALES DE ALERTA	
Estudiante que ha sido Ciberagredido	**Estudiante que está Ciberagrediendo**
• Dejar de usar repentinamente sus dispositivos y/o el internet.	• Apagar o esconder dispositivos o pantallas cuando se acerca otra persona.
• Mostrar nerviosismo o alteración al ver sus dispositivos.	• Usar dispositivos en altas horas de la noche.
• Mostrar incomodidad por ir al colegio o salir.	• Molestarse mucho si no pueden usar sus dispositivos.
• Estar de mal genio, con enfado, aburrimiento, frustración, después de estar en línea o usar redes.	• Reírse excesivamente al usar dispositivos y no compartir con personas a su alrededor el chiste.
• Dormir mucho o dormir menos de lo usual.	• Evitar hablar sobre lo que se está haciendo en línea.
• Comer mucho o menos de lo habitual.	• Retirarse o aislarse cada vez más de la familia.
• Aislarse de manera anormal, de amigos y familia.	• Tener muchas cuentas en línea o cuentas que no son propias.
• Hacer insinuaciones o comentarios repentinos sobre suicidio o falta de sentido de la vida.	• Mostar cada vez más problemas de comportamiento o quejas escolares de indisciplina.
• Perder interés por actividades, personas o cosas que antes importaban mucho.	• Mostrar preocupación excesiva por su popularidad, su estatus y su aceptación en un grupo social.
• Evitar hablar sobre lo que hace en línea.	• Mostrar incremento en insensibilidad hacia otros.
• Llamar o mandar mensajes desde colegio de querer ir a casa por enfermedad o malestar.	• Empezar a compartir con gente inadecuada.
• Preferir repentinamente estar más tiempo con padres que con pares.	• Demostrar tendencias violentas

SEÑALES DE ALERTA	
Estudiante que ha sido Ciberagredido	**Estudiante que está Ciberagrediendo**
• Mostrar reserva inusual cuando se han tenido actividades en línea .	• Ufanarse y presumir de sus habilidades digitales .
• Mostrar iras inesperadas e inexplicables.	
• Tener de repente notas bajas y no realizar trabajo escolar.	
• Abusar repentinamente de drogas y alcohol .	
• Tener mayor vergüenza, miedo, ansiedad, depresión y baja autoestima.	

Adaptado de Hinduja & Patchin, 2018; Mueller (sf).

Los anteriores factores de riesgo y de protección referidos a posibles involucramientos de los escolares en el ciberacoso son de utilidad para que Institución, Docentes y Familias estén alertas a ellos. Las situaciones de riesgo han de enfrentarse de manera eficaz, lo que implica abordaje focalizado en su reconocimiento, comprensión y manejo, que suponen atención y sensibilidad ante señales de alerta tempranas, para adoptar acciones que eviten o minimicen sus impactos y efectos (D. Pepler, comunicación personal, 11, 01, 2020). De igual manera, como se ha reiterado, tiene que ver con el fortalecimiento de protectores que, han de ser seleccionados para condiciones, situaciones y personas específicas. Por tanto, desde la comunidad escolar es fundamental la lectura de contexto, desde la cual se priorizarán los riesgos de mayor incidencia y así mismo los protectores a promover o fortalecer. Importante a la vez nutrir las miradas contextuales con información disponible basada en evidencia, sea esta gubernamental o procedente de fuentes científicas confiables, que aporta lecciones aprendidas al respecto.

Los cursos de acción frente a los riesgos para la ciberconvivencia y el uso de las Tics no son fórmulas exactas, si no que requieren como se dijo, contextualización, análisis juiciosos y planeación de acciones responsivas a las necesidades emergentes. Este abordaje preventivo en continuidad con lo planteado para la promoción de ciberconvivencia, necesariamente incluye acciones para determinar cuáles son, por qué son riesgos o protectores -en consideración de sus posibles efectos-, cómo manejarlos y adicionalmente, cómo informarlos a otras instancias o personas cuando las condiciones lo ameriten, es decir complementación de información y competencias de acción tecnológicas y socio-emocionales pertinentes a tales riesgos y protectores.

Importante aquí también no perder de vista el enfoque de curso de vida dado el uso diferencial de recursos y dispositivos tecnológicos, tanto por su acceso como por los fines que se persiguen con estos, lo cual lleva a proyectar acciones protectoras acordes con los momentos de construcción de su ciudadanía digital, y sus propias competencias cognitivas, socio-emocionales y técnicas (Kowalski et al., 2019; COST IS 0801, 2013; P. Orpinas, comunicación personal, 09, 17, 2020; Queensland Anti Ciberbullying bullying Task Force, 2018).

Es pertinente reiterar que particularmente el fortalecimiento de competencias socio-emocionales de los educandos, se apoya en lo que la IE ha venido desarrollando como parte de su compromiso con la convivencia y lo que se requiere es especificar su uso en situaciones de interacción con el mundo digital.

3.3. Acciones pedagógicas de prevención.

3.3.1. Acciones pedagógicas de prevención para Directivos Institucionales y Comité de Convivencia.

En continuidad con las acciones propuestas para la promoción de la ciberconvivencia, para los Directivos Docentes y el Comité de Convivencia se sugiere,

a. Tener información basada en evidencia sobre riesgos y protectores relacionados con el uso de las Tics, especialmente los referidos a la ciberconvivencia y los delitos tecnológicos.
b. Construir con Docentes, Familias y Estudiantes el perfil institucional sobre riesgos y protectores de la ciberconvivencia y uso adecuado de tecnología digital.
c. Determinar con instancias correspondientes, cuáles de los riesgos y protectores deben ser asumidos por la institución educativa, al contar con la competencia y los insumos requeridos para ello.
d. Propiciar aproximaciones evaluativas que den cuenta del estado previo de riesgos y protectores institucionales, antes de la realización de acciones, a fin de determinar posteriormente su efecto de cara a mantenerlas o modificarlas.
e. Reconocer y gestionar insumos tecnológicos que protejan y prevengan a la comunidad escolar de riesgos y amenazas a la integridad personal y la ciberconvivencia.
f. Concertar las formas con las que institucionalmente se dará fortalecimiento de la comunidad escolar frente a situaciones de riesgo para ciberconvivencia y el uso de las Tics.
g. Verificar el uso del perfil institucional de riesgos y protectores, en la proyección y ejecución de acciones y proyectos.
h. Indicar la integración de acciones para la protección de riesgos digitales, en los planes, proyectos y acciones institucionales para la convivencia.
i. Conformar grupo institucional de “expertos tecnológicos” para el apoyo a las acciones de soporte en el reconocimiento y manejo de riesgos, que sean requeridas por los miembros de la comunidad escolar.
j. Facilitar tiempo y recursos para la complementación de la formación y actualización sobre protectores, reconocimiento de riesgos en línea y sus manejos, al personal docente y de apoyo.
k. Proveer espacios curriculares constantes para el fortalecimiento de la ciberconvivencia con los estudiantes.
l. Propiciar incentivos para desarrollar campañas que, usando recursos tecnológicos, informen sobre riesgos y amenazas para la ciberconvivencia e integridad personal y de otros, y, sobre estrategias eficaces para reconocerlas y manejarlas.

m. Vincular a las familias en la planeación y realización de las acciones institucionales para la prevención y manejo de riesgos en la ciberconvivencia y los otros riesgos en el uso de las Tics.
n. Dar protagonismo a los estudiantes, en la planeación y realización de las acciones institucionales para la prevención de amenazas a la ciberconvivencia y demás riesgos en el uso de las Tics.
o. Otorgar reconocimientos institucionales de acciones estudiantiles protectoras de los riesgos para la ciberconvivencia y demás riesgos en línea.
p. Acudir a los aliados tecnológicos, para realizar acciones de fortalecimiento de la comunidad educativa, en la prevención y manejo de los riesgos digitales, cuando institucionalmente no se cuente con la capacidad para hacerlo o cuando se quieran fortalecer las acciones institucionales desarrolladas.
q. Planear y ejecutar difusión de los protocolos institucionales para la atención a situaciones que atentan contra la ciberconvivencia y los delitos informáticos, en que se detallen las situaciones en línea consideradas Tipo I, II o III, maneras de informarlas, las estrategias de manejo, sus actividades y momentos, los responsables de ello y las consecuencias de diversa índole para los involucrados.

3.3.2. Acciones pedagógicas de prevención para Docentes

Para los propios Docentes

En este nivel de intervención se busca principalmente que los Docentes fortalezcan sus competencias básicas señaladas para la promoción de la ciberconvivencia, refinando sus conocimientos y estrategias para detectar y manejar eficazmente los riesgos a los que sus estudiantes pueden ser o están siendo expuestos, vinculando para ello a institución, familias y especialmente a estudiantes mismos (Queensland Anti Ciberbullying Task Force, 2018; COST IS 0801, 2013; Unicef- Gobierno Provincia de Buenos Aires, 2017).

Para ellos se propone,

3.3.2.1. Para los propios docentes:

a. Revisar y contrastar con evidencia científica y empírica disponible, sus creencias y actitudes sobre los riesgos digitales propios y de sus estudiantes.
b. Adquirir o complementar su información sobre riesgos en el uso de las Tics y formas eficaces de enfrentarlos.
c. Fortalecer competencias técnicas para manejar situaciones en línea de riesgo, propias y de sus estudiantes.
d. Adoptar el abordaje de riesgos desde una perspectiva de oportunidad de fortalecimiento y preparación, para convivir en el mundo digital.
e. Participar en la planeación y desarrollo de acciones institucionales para la prevención y manejo de los riesgos en línea.
f. Conocer los protocolos institucionales para la atención a situaciones en línea que inciden en la convivencia.

3.3.2.2. Con los estudiantes:

Se resalta nuevamente la importancia de fomentar clima de confianza facilitador de la comunicación en el aula. Además, apoyarse en las competencias cognitivas, técnicas, socio-emocionales y ciudadanas fortalecidas en la promoción de la ciberconvivencia. Mantener perspectiva de curso de vida de sus estudiantes, adaptando la información y formación en competencias concretas para las necesidades propias de su desarrollo y su tipo de exposición a las TIC.

a. Ser modelo del reconocimiento y manejo de riesgos involucrados en el uso de las Tics.
b. Instigar postura de reto positivo para movilizar estudiantes a enfrentarlos y no a temerles sin actuar para protegerse.
c. Incentivar en las asignaturas y actividades a cargo, el reconocimiento de riesgos y amenazas digitales a las que pueden estar expuestos sus estudiantes, al explorar, generar o compartir información.
d. Explorar y complementar la información de los estudiantes sobre los riesgos asociados al uso de tecnología digital, mediante análisis de casos, videos, películas, noticias e información circulando en las redes.
e. Analizar con los estudiantes las razones por las cuales las situaciones reconocidas se constituyen en riesgos o amenazas al bienestar personal o colectivo, fomentando el uso del pensamiento crítico, en situaciones de la vida real o en su defecto, en videos o películas.
f. Ayudar a sus estudiantes a esclarecer las razones personales, las motivaciones, emociones, creencias y expectativas, por las cuales se ven involucrados en los riesgos digitales.
g. Explorar con los estudiantes, la responsabilidad personal que pueden tener en las diferentes situaciones de riesgo digital, al exponerse innecesariamente a ellas, involucrarse como participantes activos y al no buscar la ayuda o la información pertinente cuando la situación lo requiera.
h. Resaltar la responsabilidad moral de estudiantes, con las consecuencias sobre otras personas, conocidas o no, de sus acciones digitales.
i. Reiterar con estudiantes su participación activa en las situaciones de ciberacoso, al comentar, aprobar, etiquetar, postear o compartir la información ofensiva verbal o gráfica sobre otra persona.
j. Explorar si las y los estudiantes tienen información sobre las consecuencias personales, institucionales y legales que puede acarrear el ser partícipes de situaciones de vulneración en línea del derecho a la intimidad, honra y el buen nombre de otras personas.
k. Verificar con estudiantes la información sobre protocolos y rutas de atención institucionales frente a situaciones de ciberacoso y delitos tecnológicos, usando situaciones simuladas.
l. Enfatizar con los estudiantes, el reconocimiento de los efectos emocionales que la exposición a los diferentes riesgos puede producir en sí mismos y en otros involucrados en las situaciones de riesgo.
m. Sensibilizar a los estudiantes en la compasión requerida para considerar los efectos emocionales que se producen al resultar involucrados en las situaciones de riesgo digital.

n. Recordar el carácter permanente de la información buscada y compartida por medios tecnológicos, y cómo esta va configurando la huella digital en línea de sus estudiantes.
o. Fortalecer en sus estudiantes, la consideración previa de consecuencias personales y colectivas, a nivel inmediato y a largo plazo, de las acciones que piensan llevar a cabo en línea, a fin de tenerlas en cuenta antes de realizarlas.
p. Determinar las competencias técnicas y socio-emocionales de los estudiantes en el manejo de los riesgos asociados al uso de tecnología digital, usando situaciones simuladas en las que ellos puedan verse involucrados.
q. Construir con los estudiantes un inventario de recursos y necesidades a nivel de información y formación en competencias, que los grupos requieren para fortalecerse ante los riesgos en el uso de las TICS.
r. Propiciar que los estudiantes elaboren sus propios planes de acción para el fortalecimiento ante los riesgos digitales, teniendo en cuenta sus propios recursos y los institucionales.
s. Apoyar a estudiantes digitalmente muy competentes, para asumir liderazgo en los planes grupales de fortalecimiento ante riesgos digitales.
t. Apoyar a los estudiantes en acciones de ciberseguridad con sus contraseñas, cuentas, perfiles, e información privada.
u. Determinar con los estudiantes cuándo son requeridos apoyos de aliados técnicos expertos, para el fortalecimiento de sus estrategias de protección, a fin de gestionarlos con la institución.
v. Inducir a la generación de propuestas sobre cómo vincularse al fortalecimiento institucional de padres, estudiantes y docentes, frente a los riesgos asociados a la cibertecnología.
w. Ayudar a que los estudiantes construyan su propio kit de herramientas para enfrentar las ciberamenazas.
x. Instar a los estudiantes a la elaboración de material digital que pueda ser usado para alertar y fortalecer a la comunidad educativa frente a los riesgos digitales.

3.3.2.3. Con las familias

a. a. Propiciar espacios de encuentro para determinar recursos y necesidades familiares frente al reconocimiento y manejo de los riesgos en el uso de las TIC.
b. Reiterar con los padres, la importancia de mantener la alianza con la escuela para unir esfuerzos que potencien la protección de estudiantes frente a riesgos y amenazas digitales.
c. Informar a instancias de coordinación y /o Comité de Convivencia, sobre recursos y necesidades parentales para el apoyo de los niños, niñas, adolescentes y jóvenes frente a los riesgos digitales, de cara a la generación de acciones de la institución.
d. Trabajar con las familias en la generación y ejecución de planes para el fortalecimiento de competencias frente a los riesgos personales y de los niños, niñas, adolescentes y jóvenes con la cibertecnología.
e. Propiciar encuentros para reconocer, reflexionar y re- evaluar creencias y actitudes sobre riesgos digitales de los niños, niñas, adolescentes y jóvenes, para que sean acordes con la realidad y puedan articularse con las acciones que se proyecten para fortalecerlos frente a ellos.

f. Enfatizar con las familias la relevancia de la orientación y acompañamiento a los niños, niñas, adolescentes y jóvenes en su vida digital y, en el reconocimiento y manejo de los riesgos involucrados en ella.
g. Sensibilizar a las familias en la importancia de fortalecer a los niños, niñas, adolescentes y jóvenes frente a los riesgos digitales, en lugar de atemorizarlos para que actúen desde el miedo y la amenaza.
h. Recordar a las familias la importancia de adecuar sus acciones protectoras al momento de curso de vida de sus niños, niñas, adolescentes y jóvenes, teniendo en cuenta riesgos diferenciales acordes con su exposición y usos de la tecnología digital.
i. Reiterar con las familias la necesidad de controlar en los más pequeños, dispositivos, acceso, tiempos y contenidos, a la vez que se les ayudan a fortalecer competencias personales que les permitan disfrutar de opciones tecnológicas al tiempo que reconocen y enfrentan los riesgos digitales.
j. Señalar a las familias relevancia de reconocer en los adolescentes y jóvenes, las necesidades específicas frente a los riesgos tecnológicos que pueden enfrentar, y el rol parental de orientación y acompañamiento no prohibitivo ni invasivo, en el fortalecimiento de sus competencias personales y tecnológicas frente a ellos.
k. Instar a que las familias trabajen conjuntamente en el reconocimiento de los riesgos digitales y en el fortalecimiento de estrategias para su manejo eficaz, de acuerdo con las necesidades de cada miembro.
l. Orientar a las familias en la importancia de reflexionar con los niños, niñas, adolescentes y jóvenes sobre por qué se consideran riesgosas algunas situaciones en línea, teniendo en cuenta los efectos que se puedan producir en sí mismos y en otras personas vinculadas a ellas.
m. Inducir a que las familias aborden con los niños, niñas, adolescentes y jóvenes, las responsabilidades personales que tienen frente a los riesgos cibernéticos, exponiéndose a ellos, vinculándose a las situaciones y dejando de buscar información adicional o ayuda en situaciones que lo ameriten.
n. Insistir con las familias en la necesidad de vincular los valores familiares y el respeto por los derechos propios y de otros, en el reconocimiento y manejo de las situaciones riesgosas en línea que puedan enfrentar niños, niñas, adolescentes y jóvenes.
o. Alentar y facilitar en las familias el fortalecimiento de prácticas de crianza sensibles, cálidas y responsivas, en las que se hable de riesgos y amenazas en las TIC, y se expresen libremente posturas, temores y acciones al respecto.
p. Fomentar que los padres concedan rol protagónico a sus niños, niñas, adolescentes y jóvenes, en las acciones proyectadas para reconocer y enfrentar riesgos digitales, apoyándose en sus destrezas tecnológicas.
q. Informar sobre protocolos, rutas de atención y estrategias institucionalmente establecidas para hacer frente a las situaciones con los estudiantes al verse involucrados en riesgos y ciberamenazas.

3.3.3. Acciones pedagógicas de prevención de los estudiantes

Enfatizando el rol de agentes de su vida digital por parte de los estudiantes, cabe destacar posibles acciones para su fortalecimiento frente a situaciones en línea riesgosas para sí mismos o, para otros involucrados en las situaciones (D. Pepler, comunicación personal, 11, 01, 2020; M. Garaigordobil, comunicación personal, 09, 23, 2020; P. Orpinas, comunicación personal, 09, 17, 2020; R. Slaby, comunicación personal, 09, 21, 2020; R. Thornberg, comunicación personal, 10, 12, 2020).

Para ellos se sugiere

a. Revisar sus conocimientos y competencias técnicas y socioemocionales, para el reconocimiento y manejo de los riesgos digitales que pueden enfrentar.
b. Recordar implicaciones personales, sociales, escolares y legales que pueden darse al exponerse a diversos tipos de ciber riesgos.
c. Tener en cuenta lo que la Ley 1620 y el Decreto 1965 de 2013, establecen como situaciones en línea Tipo I, II y III, los procesos de atención y sus consecuencias, para reconocer formas de verse involucrados en ellas.
d. Establecer su propio perfil de cuáles son las competencias digitales y socioemocionales en las que son muy fuertes, y aquellas que deben fortalecer, para hacer frente a las situaciones amenazantes en línea.
e. Delinear posibles acciones para fortalecer sus competencias al afrontar eficazmente riesgos cibernéticos.
f. Reflexionar sobre por qué las situaciones pueden considerarse riesgosas, teniendo en cuenta posibles efectos personales y sobre otros involucrados, que se puedan presentar.
g. Analizar las razones que los inducen a exponerse a los riesgos en el uso de las TIC.
h. Recordar su responsabilidad personal en las situaciones digitales riesgosas, por exponerse a ellas, participar activamente y, no buscar la ayuda o información adicional cuando lo amerite la situación.
i. Tener en cuenta que, en las situaciones de ciberacoso, son participantes activos cuando comentan, aprueban, etiquetan, postean y comparten agresiones, ofensas o exclusiones a otra persona, verbales o gráficas.
j. Tener claro que, a pesar del anonimato en las redes, sus acciones con otras personas y las consecuencias para ellas son su responsabilidad.
k. Recordar que el derecho a la protección de la integridad, la dignidad, la privacidad, la honra y el buen nombre, también operan en línea.
l. Usar el pensamiento crítico frente a la información en línea a la que se exponen, para determinar su veracidad o falsedad y para considerar las consecuencias posibles de comentarla, aprobarla y compartirla.
m. Reconocer y regular las emociones que les suscita la información en línea, antes de dar respuestas a la misma, para evitar actuar de manera impulsiva teniendo consecuencias indeseables perdurables a futuro.
n. Cuidar su información personal y privada, evitando que sea accesible a otras personas sin su consentimiento.
o. Evaluar antes de subir información a las redes, posibles efectos para su imagen personal a mediano y largo plazo.

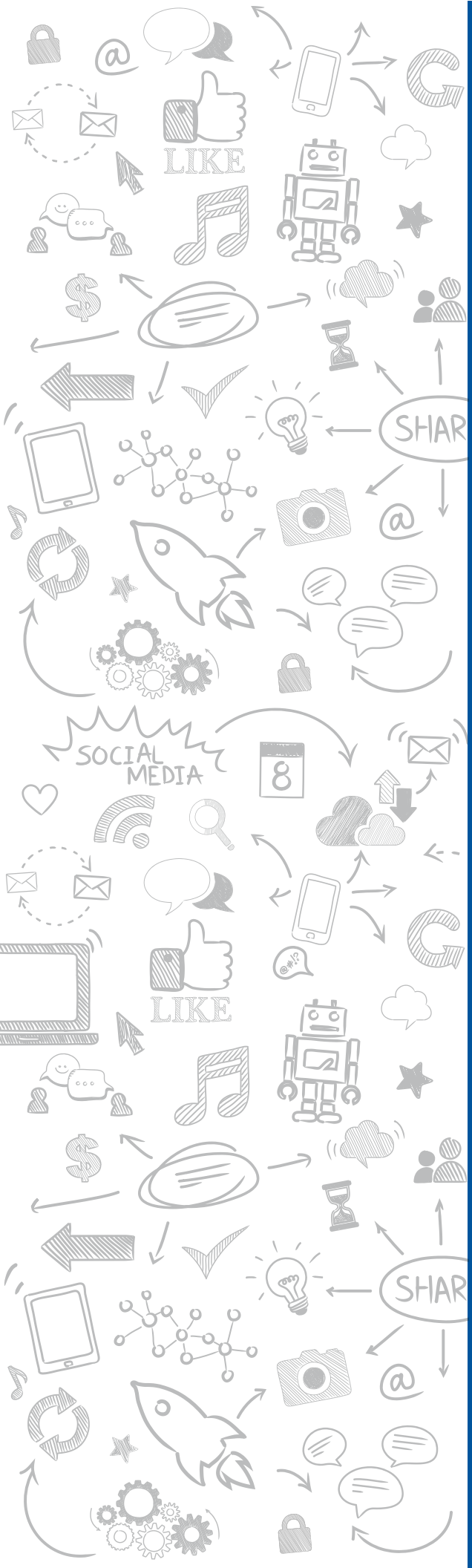
p. Analizar contactos en línea, antes de compartir información personal o concertar encuentros con ellos.
q. Reconocer efectos de presiones grupales en la exposición y manejo de situaciones de riesgo en línea.
r. Concertar con los pares, estrategias de fortalecimiento grupal frente a los riesgos digitales.
s. Acordar con compañeros maneras de parar agresiones digitales y de acompañar a compañeros afectados, aunque no sean parte de su grupo de amigos más cercanos.
t. Proponer acciones y estrategias de fortalecimiento institucional de respuesta a riesgos cibernéticos en las que puedan involucrarse.

Tabla 10. Imaginarios y realidades sobre riesgos en línea de escolares

Imaginarios	Realidades
• Toda conducta en línea de escolares es una conducta de riesgo	• FALSO. Hay conductas en línea que contribuyen con el aprendizaje, la socialización, la creatividad y la sana diversión.
• La exposición de escolares a las pantallas siempre produce efectos negativos.	• FALSO. La exposición a pantallas con tiempo dosificado según edad, y acceso a contenidos adecuados no produce efectos negativos.
• La mayor parte de padres o cuidadores desconoce las actividades en línea de escolares.	• VERDADERO. La falta de familiaridad de adultos con las tecnologías digitales y el acceso de escolares a sus propios dispositivos y cuentas en redes sociales hacen más probable que los cuidadores desconozcan sus actividades en línea.
• Toda exposición a riesgos digitales produce daños a escolares.	• FALSO. Algunos escolares logran evadirlos o enfrentarlos adecuadamente.
• El uso de dispositivos digitales cada vez ocurre a edades más tempranas.	• VERDADERO. Cada vez son más usados los dispositivos digitales como medio de entretenimiento para infantes y pre- escolares. Y, a edades más tempranas se les proporcionan los dispositivos digitales
• El uso de redes convierte a escolares en ciberacosadores.	• FALSO. Las razones por las que se agrede a un par en línea son varias y, muchos escolares hacen buen uso de las redes fortaleciendo sus intercambios sociales.
• El anonimato, el estar “ocultos” tras pantallas hace que escolares agredan más fácilmente a otros pares.	• VERDADERO. El no darse cuenta de los efectos de conductas agresivas sobre personas agredidas y, el poder ocultar la identidad hacen más posible la agresión en línea.
• Prohibir a escolares uso de dispositivos y redes es la mejor manera de protegerlos de los riesgos en línea.	• VERDADERO. Prohibir a escolares uso de dispositivos y redes es la mejor manera de protegerlos de los riesgos en línea.
• La publicación de fotos y videos personales hace que escolares sean fácilmente presas de ciberagresores y depredadores sexuales adultos.	• FALSO. Existen opciones de seguridad que permiten compartir dichas imágenes solo con personas conocidas.

Imaginarios	Realidades
• Lo que escolares publican, comparten y a lo que acceden en línea, construye su huella digital personal.	• VERDADERO. La propia actividad digital es una manera de mostrar quienes somos, es parte de la identidad digital.
• Existen unas “buenas maneras” para relacionarse en línea.	• VERDADERO. La “Netiqueta” es el código de buenas maneras y de respeto en línea construido por los propios usuarios.
• Desde edades tempranas se puede educar a escolares en buen uso de recursos digitales.	• VERDADERO. La educación digital debe comenzarse tempranamente generando hábitos de uso adecuados que en edades posteriores se irán complementando con herramientas de protección frente a posibles riesgos en línea.

Adaptada de Common Sense Media, 2020; ICBF, 2019; Hinduja, 2020; Hinduja & Patchin, 2020; Unicef, 2019.



Del Componente de Atención

4. Del componente de atención.

Como se ha explicado, las situaciones de ciberconvivencia se encuentran referidas en la Ley 1620 de 2013 y, por tanto, su manejo se enmarca en los principios que orienta dicha ley y su decreto reglamentario, así como en los principios dados por las normas conexas: Ley General de Educación (1994), Código de Infancia y Adolescencia (2006), Ley de delitos informáticos (2009). En este sentido, habrá de tenerse en cuenta, que el manejo de las diferentes situaciones estará dado desde el marco de la justicia restaurativa, por cuanto el fin, es reparar los daños causados a estudiantes involucrados, promover aprendizajes que transformen el comportamiento inadecuado y así lograr la no repetición de los hechos, principalmente, de aquellos que constituyen prácticas de ciberacoso o delitos informáticos.

La atención a situaciones de estudiantes relacionadas con el uso de las TIC también implica miradas exhaustivas, analíticas, cuidadosas, articuladas con las normas vigentes en materia de educación y específicamente de convivencia escolar, los protocolos y proyectos institucionales, el Manual de Convivencia, para la implementación de acciones claras y concretas, en las que se evidencie de manera contundente para la comunidad escolar involucrada y para los restantes miembros de esta que tienen acceso a información sobre dichas situaciones, que hay una postura institucional frente a ellas, que se han generado estrategias y acuerdos para su abordaje, y que se procede de manera articulada a fin de que tales situaciones sean oportunidades de aprendizaje desde las cuales los involucrados se fortalecen como personas y ciudadanos.

La atención a las situaciones digitales que afectan a estudiantes debe ser asumida por el EE, independientemente que sean o no realizadas en el contexto físico y en los horarios escolares. Se asume como una situación de ciberacoso escolar y delito informático, a toda aquella situación que emerge en el marco de una relación originada desde el quehacer y la cotidianidad escolar. El hecho de que haya al menos un estudiante involucrado lo amerita, tal como se establece en el Decreto 1965 de 2013. Además del compromiso normativo, atender estas situaciones proporciona a la comunidad escolar sentido de seguridad en términos de que la institución realmente orienta y acompaña, protege, cuida, con lo cual se incrementa su sentido de pertenencia, lo que a la vez afecta positivamente la convivencia escolar.

4.1. Clasificación de situaciones digitales

La atención a situaciones digitales evidentemente está enmarcada desde la Ley 1620 de 2013, su Decreto Reglamentario 1965 y así mimo, ilustrado su abordaje en la Guía 49 (Ministerio de Educación Nacional, 2013), por lo cual, al igual que todas las situaciones que alteran la convivencia escolar, las situaciones conflictivas que tienen lugar en el espacio virtual y que se presentan entre escolares o que les afectan, se clasifican en situaciones Tipo I, II y III y acorde a ello, o bien son del manejo del EE y las familias de los involucrados, o bien, según el tipo, implican el concurso y la colaboración de las instituciones garantes y protectoras. El propósito de dicha clasificación es orientar respecto los responsables del manejo y las acciones óptimas para solucionar cada situación desde una perspectiva de justicia restaurativa que parte desde el interés superior de niños, niñas y adolescentes.

Este propósito dista del uso de la diferenciación como herramienta para determinar el tipo de castigo o sanción que se usará para estudiantes responsables, porque el espíritu subyacente es educativo no punitivo, sin que ello implique carencia de consecuencias, asunción de responsabilidades, y, acciones de reparación y restitución por las ciberagresiones. La diferenciación de cibersituaciones no es parte de un sistema penal acusatorio, es integrante de un proceso educativo en el que estudiantes que han sido agresores, agredidos, observadores y la comunidad escolar en pleno, las convierten en experiencias significativas para el aprendizaje de la convivencia y la ciudadanía y, en particular de la ciberconvivencia y la ciudadanía digital. Busca igualmente identificar los actores con competencia en la solución de las situaciones de cara a la garantía y restitución de los DDHH, DHSR de NNAJ toda vez que éstos hayan sido vulnerados a través de las relaciones virtuales.

4.1.1. Cibersituaciones Tipo I.

Se consideran cibersituaciones Tipo I, todos aquellos conflictos que ocurren entre estudiantes, en el marco de interacciones mediadas por las TIC, que no se han hecho públicos a través de las redes, que no han sido sistemáticos ni recurrentes entre los involucrados y que además entre los implicados existe, relativamente, una relación simétrica de poder, es decir, no hay una relación de abuso de uno hacia el otro. Entre estas se encuentran:

- Agresiones digitales, mensajes, memes, imágenes o correos electrónicos insultantes u ofensivos, que buscan afectar negativamente a la otra persona (Decreto 1965, Artículo 30).
- Conflictos (diferencias, disputas, malentendidos) que se han suscitado por interacciones virtuales: apodos, burlas, bromas insultantes, trato agresivo o descalificante; o en su defecto, ignorar las demandas de interacción o de respuesta a las publicaciones que uno de los implicados hace.
- Las agresiones digitales pueden ser mutuas, o de una de las partes hacia la otra.
- Las agresiones si bien se realizan por medios digitales, no han sido difundidas a través de redes, aplicaciones o plataformas.
- Se carece de antecedentes de acoso escolar cara a cara, entre personas involucradas.
- Las agresiones digitales no han producido daño a la integridad y el bienestar físico o emocional de las personas involucradas, generando condiciones de incapacidad (Decreto 1965 de 2013, Artículo 40).

4.1.2. Cibersituaciones Tipo II.

Las cibersituaciones tipo II, corresponden básicamente a situaciones de acoso escolar, y a conductas de riesgo que se dan a través del uso de las TIC, que involucran a escolares y ponen en riesgo su integridad moral o física.

Se concibe como cibersituaciones Tipo II, todas aquellas prácticas que afectan o podrían llegar a afectar significativamente la salud mental y física de los estudiantes: sexting, pishing, contactos con extraños y que se realizan de manera frecuente.

Son prácticas de ciberacoso: agresiones digitales, mensajes, memes, imágenes o correos electrónicos insultantes u ofensivos, burlas, ridiculizaciones, humillaciones, trato despectivo, degradación, intimidación, exclusión, rechazos a compañeros escolares que buscan afectar

negativamente a la otra persona (Decreto 1965, Artículo 30) y que se hacen públicas a través de las TIC y especialmente en las redes sociales. También son conductas de ciberacoso, cualquier forma digital repetida de agresión, persecución, que un par escolar comete hacia otro, aunque no se haya hecho pública.

Cabe señalar que se determina como situación de ciberacoso, toda conducta hostil y agresiva que se publica a través de redes sociales, aunque sea la primera vez que se presenta, puesto que la condición de repetición de las acciones agresoras -necesaria para ser considerado acoso-, está dada por la difusión ilimitada e incontrolable de las agresiones a través de las TIC. De igual manera, otra de las condiciones, la asimetría relacional también está incluida debido a la indefensión de agredidos, en este caso por su incapacidad para poner fin a la difusión en línea de mensajes en su contra, la condición 24/7 de circulación de los mensajes, y en muchas ocasiones, el desconocimiento de la procedencia de acciones cibernéticas en su contra.

El ciberacoso produce daños a las personas agredidas, al impactar negativamente su bienestar, las relaciones sociales, la convivencia, la estima personal, el rendimiento académico entre otros, sin generarles condiciones de incapacidad funcional (Decreto 1965 de 2013, artículo 40). Así mismo, el ciberacoso tiene efectos negativos en estudiantes que han sido agresores. Se ha observado en ellos efectos negativos sobre sus competencias relacionales al adoptar para ellas el uso del poder y la agresión, aumentando la probabilidad futura de involucrarse en situaciones de agresión y violencia hacia los demás y la adopción de otras conductas de riesgo, tales como consumo, prácticas sexuales sin responsabilidad (D. Pepler, comunicación personal, 11, 03, 2020).

La atención de los daños causados por las cibersituaciones Tipo II –de acoso y prácticas de riesgo- no solo le compete a la comunidad educativa –docentes y familias-, sino que requiere del concurso de otras instituciones garantes tales como salud e ICBF, entre otros, según el nivel de afectación de la salud física o mental de las personas involucradas, y, la necesidad de adoptar medidas de restablecimiento de derechos.

De igual manera cabe resaltar que las acciones constitutivas de la situación Tipo II, no pueden ser correspondientes a delitos tipificados dentro de la legislatura colombiana vigente.

El ciberacoso lo constituyen,

- Humillación, ridiculización, burlas sobre compañeros, a través de mensajes explícitos, de memes, de imágenes retocadas o no, de páginas creadas para dicho propósito.
- Realización de comentarios burlescos, insultantes u ofensivos sobre compañeros, a través de redes sociales y de Apps.
- Divulgación de fotos comprometedoras para el estudiante sin su previo consentimiento.
- Envío constante de correos electrónicos o mensajes de texto ofensivos o insultantes.
- Envío insistente y sistemático de mensajes o correos electrónicos que aunque no sean insultantes, se convierten en una situación de intimidación o acoso. Estos suceden principalmente con intenciones de galanteo o coqueteo pero también pueden surgir en el marco de relaciones de amistad.
- Exclusión intencional de pares escolares, de un chat, red social o plataforma.

• Grabación sin consentimiento de situaciones socialmente embarazosas o íntimas en las que ha estado la persona agredida, difundidas posteriormente a través de las redes.
• Publicación sin consentimiento de mensajes personales previamente intercambiados entre la persona agredida y el agresor u otras personas.
• Denigración sexista, clasista, xenófoba, política o religiosa a través de TIC, que ocurre entre compañeros escolares.
• Chantaje emocional para que el par escolar, en nombre de la amistad o el noviazgo le dé claves de acceso a cuentas personales.
• Chantajes y amenazas a través de las TIC para obligar al par escolar a realizar acciones en contra de su voluntad (tareas, guardar silencio o reserva sobre algún secreto, foto o vídeo comprometedor).

Entre las cibersituaciones tipo II que corresponden a las prácticas de riesgo mediadas por las TIC, se encuentran:

• Citaciones a agresiones por medio de las TIC: pactar una pelea a la salida de la jornada escolar; incitar peleas a través de las TIC.
• Sexting: intercambio de fotos personales de desnudos o semidesnudos, de fotos eróticas.
• Uso excesivo de las TIC que denotan un comportamiento adictivo, y, rechazo o apatía a las relaciones presenciales.
• Establecimiento de contactos con desconocidos: apps para establecer relaciones de amistad, pareja, intercambios sexuales entre pares escolares que no involucra a menores de 14 años.
• Intercambio de pornografía.

4.1.3. Cibersituaciones Tipo III.

Corresponden a este tipo las situaciones de ciber agresión escolar que sean constitutivas de presuntos delitos contra la libertad, integridad y formación sexual, referidos en el Título IV del Libro 11 de la Ley 599 de 2000, o que constituyen cualquier otro delito establecido en la ley penal colombiana vigente (Decreto 1965 de 2013, artículo 40).

• Suplantación de identidad, haciéndose pasar por la persona agredida, para realizar acciones digitales inadecuadas.
• Hackeo de las claves. Este hackeo no implica suplantación de identidad, sino intromisión en documentos privados, tales como el correo.
• Suplantación de las cuentas de redes sociales o hackeo de claves y suplantación de identidad hacia otros pares escolares o hacia los docentes.
• Grabación sin consentimiento de situaciones socialmente embarazosas o íntimas en las que ha estado la persona agredida.
• Difamación contra la honra y el buen nombre del estudiante, difundida a través de las TIC. Entre estas se encuentra: acusaciones de hechos delictivos, divulgación de información personal –hechos penosos o embarazosos-, publicación de mensajes íntimos, fotos o vídeos previamente intercambiados entre la persona agredida y el agresor u otras personas.

• Extorsión y amenazas contra la vida, ejercidas a través del uso de las TIC.
• Todos aquellos delitos sexuales que se puedan incitar, iniciar a través de las TIC y en las que los estudiantes se vean afectados. Aunque los delitos sexuales inducidos o iniciados a través del uso de las TIC, no sucedan entre pares escolares, le compete a todos los adultos de la comunidad educativa, activar la ruta para garantizar la protección de niños, niñas, adolescentes y jóvenes que se vean afectados. Entre estas situaciones se encuentran:

- Intercambio de pornografía entre escolares menores de 14 años; incitación a la prostitución a menores de edad.
- Incitación de un adulto – docente, directivo y otro miembro del EE- hacia los estudiantes: invitaciones a salidas privadas, mensajes de coquetería o galanteo, insinuaciones sexuales.

4.2. Atención a situaciones digitales Tipo I.

Las acciones enmarcadas como correspondientes a situaciones digitales Tipo I, al trasladarlas al plano de la convivencia presencial, son homologables a situaciones de conflicto manejado de manera inadecuada, que por tanto incluyen agresiones en este caso digitales, sean estas entre las partes en conflicto, de una parte, a otra que no responde a la ciberagresión, o, agresiones digitales que se producen como única vez. Frente a estas situaciones digitales Tipo I entonces, tal como se estipula en el Artículo 42 del Decreto 1965, no hay en primera instancia intervención por parte de los Directivos institucionales o Directivos docentes, tampoco del Comité de Convivencia o de las familias, y lo procedente es la mediación, tendiente al reconocimiento de la situación como conflicto, y conexo a ello, la búsqueda de soluciones concertadas que, restableciendo las relaciones entre las partes, eviten el escalamiento a agresiones de mayor severidad y así mismo la repetición, mediación que debe realizarse por parte del Docente que tiene información sobre la situación (Ley 1620, de 2013) o, por un par mediador, debidamente capacitado.

Como se ha explicado, las situaciones de ciberconvivencia se encuentran referidas en la Ley 1620 de 2013 y por tanto, su manejo se enmarca en los principios que orienta la ley y su decreto reglamentario, así como en los principios dados por las normas conexas: Ley de Educación, Ley de Infancia y Adolescencia, Ley de Delitos informáticos. En este sentido, habrá de tenerse en cuenta, que el manejo de las diferentes situaciones estará dado desde el marco de la justicia restaurativa, por cuanto el fin, es reparar los daños causados a estudiantes involucrados, promover aprendizajes que transformen el comportamiento inadecuado y así lograr la no repetición de los hechos, principalmente, de aquellos que constituyen prácticas de ciberacoso o delitos informáticos.

Desde este orden de ideas, la atención a las situaciones conflictivas de ciberconvivencia inicia con el proceso de gestión interinstitucional que compete a la conformación, reglamentación y gestión de los Comités Escolares de Convivencia y al respectivo ajuste de los Manuales de Convivencia de cada EE, con la participación de toda la comunidad educativa, incluidos estudiantes y familias. De igual manera, de acuerdo con el tipo de situación y el nivel de afectación, la atención a casos de ciberacoso y posibles delitos informáticos les compete también a las instituciones garantes de los derechos de los derechos de NNAJ: ICBF, Comisarías de Familia, Salud, Gobierno, Deporte, Cultura, Policía de Infancia y Adolescencia, y a Personería –cuando las demás instituciones no actúen de manera oportuna.

En consecuencia, previo a determinar cómo se manejará cada una de las situaciones conflictivas de ciberconvivencia, según su tipo, es competencia del Gobierno Escolar y el Comité Escolar de Convivencia:

4.2.1. Comité Escolar de Convivencia:

a. Conformar el Comité Escolar de Convivencia; definir sus reglamentos de funcionamiento, objetivos de gestión escolar generales y plan de acción del año lectivo correspondiente, liderar la actualización del Manual de Convivencia en lo relacionado con el sistema de convivencia escolar y ciberconvivencia.
b. Definir, con el concurso de la comunidad educativa, previamente en los protocolos, guías y Manual de Convivencia, los lineamientos para el manejo institucional a dichas cibersituaciones. Determinar de acuerdo con las situaciones, quiénes serán los adultos que manejarán cada tipo de situación y capacitarles para su respectiva función. Definir la estrategia de Registro Único y Seguimiento de Situaciones que alteran la ciberconvivencia escolar. Incluir todos estos ajustes en el Manual de Convivencia.
c. Tener en cuenta al determinar quiénes serán los adultos responsables de atender las situaciones conflictivas de ciberconvivencia: el tipo de situación, los recursos institucionales generales y las características del EE donde asisten los estudiantes y se identifiquen las situaciones. Las cibersituaciones tipo I serán de la competencia del docente que identifique la situación o el docente titular. Ante cibersituaciones de Tipo II, quien atienda la situación variará; sí la IE y el EE cuentan con orientador psicosocial, esta persona será la más indicada para atender dichas situaciones, no obstante, si el EE está ubicado en una zona alejada de la sede principal lo ideal será que la situación sea atendida por el docente titular o el coordinador que esté en el EE una vez se haya identificado la situación. Las cibersituaciones Tipo III, una vez identificadas, deben ser notificadas al rector o coordinador de convivencia, quiénes deberán iniciar el proceso de activación de la ruta, sin embargo, la ubicación geográfica del EE educativo, incidirá en quién inicie el proceso de reconstrucción de la información y notificación a las familias y las entidades competentes.
d. Llevar a cabo una estrategia de difusión periódica de las normas de convivencia escolar, los protocolos de manejo de las situaciones que alteran la convivencia y ciberconvivencia escolar. Esta difusión debe vincular a toda la comunidad educativa.
e. Implementar la estrategia “Acuerdos de Convivencia y ciberconvivencia” al inicio del año lectivo, de tal manera que estudiantes y docentes comprendan y apropien las normas en su cotidianidad escolar. Esta se desarrolla con el docente titular de cada grupo escolar.
f. Acordar que la información referente a las cibersituaciones debe ser manejada de manera confidencial, solo por personas designadas para ello, cuidando que no se difunda para así preservar el derecho a la protección de la intimidad de estudiantes involucrados, evitando además situaciones que podrían agravar las circunstancias actuales.
g. Facilitar espacios formativos de estrategias de resolución de conflictos tanto para estudiantes como para los adultos del EE.
h. Verificar que los adultos a cargo cuenten con las competencias personales socioemocionales y las técnicas para el manejo de conflictos entre estudiantes.
i. Decidir si se establece un programa de Mediadores Escolares para involucrarlos en el manejo de cibersituaciones Tipo I.

j. Seleccionar la estrategia para capacitación de los Mediadores Escolares, que sea apropiada al EE, y cuyos contenidos puedan garantizar el logro de fortalecimiento de competencias socioemocionales y técnicas, requeridas para mediar situaciones de conflicto entre pares.
k. Establecer el mecanismo con el que se verificará que la estrategia de capacitación de Mediadores Escolares alcanzó los objetivos formativos acordados.
l. Promover la importancia de la confidencialidad del manejo de la información sobre las situaciones que alteran la convivencia y la ciberconvivencia escolar, de manera que solo se difunda entre quienes son delegados para su abordaje, preservando el derecho a la protección de la intimidad de estudiantes involucrados, evitando además la generación de situaciones que agraven las circunstancias actuales.

4.2.2. Para los Docentes, Orientadores o adultos delegados

Teniendo en cuenta que las situaciones conflictivas de ciberconvivencia Tipo I, corresponden a conflictos manejado de manera inadecuada, incluyen agresiones por medios digitales producidas de manera esporádica o una sola vez, que no se han hecho públicas en redes sociales y en las cuales, no hay entre implicados una relación de dominio, sumisión o abuso de poder. Estas situaciones, una vez identificadas, son del resorte del docente que tenga información sobre ella, tanto por haberla observado o por que ha recibido la información de un tercero–otro adulto del EE, estudiante, familiar o acudiente de alguno de los implicados-.

Este docente observador o informado, podrá ejercer su rol de mediador o, de acuerdo con los recursos del EE, podrá sugerir mediación por pares e incluso solicitar apoyo del orientador psicosocial o el docente orientador (Ley 1620 de 2013; Decreto 1965 de 2013).

La mediación docente, como se sabe, se dará para facilitar el dialogo y la reflexión entre involucrados en pro de lograr soluciones concertadas que permitan superar la molestia u ofensa causada, eviten el escalamiento hacia la agresión, restablezcan las relaciones y así mismo, promuevan la no repetición, es decir, el aprendizaje del comportamiento adecuado al hacerse responsables de sus actos.

La mediación, sea realizada por pares o por el docente mismo, concluirá con la definición de acuerdos negociados entre estudiantes implicados, los cuales se firmarán en un documento escrito y serán el referente para su seguimiento. En el caso en que los estudiantes se nieguen a cooperar para llegar a acuerdos concertados, el docente indicará la solución reparadora, según hayan sido los hechos y acorde a lo estipulado en el Manual de Convivencia del EE.

Cabe resaltar que al tratarse de “conflictos digitales”, que ocurren generalmente a través de los dispositivos personales de estudiantes, es altamente probable que la información respecto a la situación llegue a través de terceros o de solo una de las partes involucradas posterior a su ocurrencia, lo cual implica que en el proceso de mediación se tengan consideraciones adicionales, dependientes del escenario en el que obtiene dicha información el adulto escolar.
Importante resaltar que las acciones que se sugieren a continuación y todas las acciones que se lleven a cabo con estudiantes involucrados en cibersituaciones Tipo I, deben estar permeadas de actitudes empáticas hacia las partes, de respeto por sus puntos de vista y el dialogo debe darse en un clima cálido, de tal manera que se genere la confianza necesaria para hablar honestamente de lo sucedido.

La identificación de la situación

a. Si el docente se entera por información de un tercero, es importante determinar de qué manera tuvo acceso a la información sobre el ciberconflicto, precisar quiénes son las personas involucradas; identificar sí, conoce antecedentes de conflictos o acoso escolar presencial por parte de involucrados. Si el tercero es un estudiante, además, preguntar si está dispuesto a actuar como mediador en caso de tener el entrenamiento correspondiente y o sí, por el contrario, prefiere mantener su nombre en el anonimato.

b. Sí el docente se entera por el estudiante directamente afectado, después de escucharle y ayudarle a expresar sus emociones, es preciso motivarle para abordar la situación con demás personas implicadas, para darle manejo adecuado. Sí el estudiante acepta, se procederá a concertar objetivos, formas y momentos para el abordaje de la situación conflictiva con par o pares involucrados. En caso de una respuesta negativa, informar al estudiante cuál será el proceso a seguir para darle solución a la situación y aclararle que la información entregada será puesta en consideración con el o los otros estudiantes involucrados a fin de darle solución.

Para reforzar la implementación de la Ruta de Atención Integral:

1. Atender la situación de manera inmediata. Evitar minimizarla o restarle importancia a la misma.

2. Se recomienda siempre agradecer a la persona que notifica la situación de ciberconflicto, su aporte a la convivencia escolar, al informar sobre situaciones que la amenazan.

La mediación como proceso para la búsqueda de la solución

La atención a las cibersituaciones Tipo I busca su resolución a través de la mediación a fin de contribuir a la transformación del comportamiento inadecuado y el desarrollo de habilidades para la convivencia y ciberconvivencia. Para ello es necesario generar espacios de conciliación en los que estudiantes involucrados tengan la oportunidad de expresar libre y abiertamente sus versiones de lo ocurrido, reflexionar sobre las razones personales y de otra índole que motivaron o contribuyeron con la situación conflictiva, identificar soluciones reparadoras y lograr una solución negociada, justa, que se relacione de manera directa con los hechos y sus causas.

La pretensión de la mediación es evitar acciones mecánicas, facilitando por el contrario espacios en los que realmente se subsanen las diferencias conflictivas para así generar soluciones reales, viables y eficaces para las situaciones conflictivas.
La mediación es un proceso que implica diálogo con estudiantes implicados, de manera paulatina, iniciando –en la medida de lo posible- por la persona afectada, hasta llegar a facilitar una conversación entre todos los implicados, favoreciendo la expresión de emociones, la reconstrucción de los hechos, el reconocimiento de la causa del conflicto y de la solución al mismo y, la definición de acuerdos negociados. Estos últimos se deben registrar en el formato que haya diseñado el EE para atender las cibersituaciones Tipo I.

A lo largo del proceso de mediación, tanto en las conversaciones individuales como en la colectivas, al reconstruir la situación conflictiva, es preciso formular preguntas para recoger información que permitan precisar:

a. Quiénes son las personas involucradas en la situación de ciberconflicto.
b. Cuáles fueron las prácticas en línea que dieron origen al conflicto: cómo inició y qué reacción tuvo cada persona implicada.
c. Qué tipo de comunicación o agresión fue emitida o intercambiada en línea; de qué forma se presentó la información y con qué frecuencia ha sucedido.
d. Sí ha habido intercambio de información con otras personas adicionales a los directamente implicados en el conflicto.
e. Sí entre las personas involucradas ha habido conflictos previos o acoso escolar presencial.
f. Las consecuencias personales, sociales, escolares o de otra índole ocurridas por la situación en estudiantes involucrados.
g. Decisiones que, en lugar de ayudarles a resolver la situación, agudizaron el conflicto e incidieron negativamente en el propio bienestar, en su relación interpersonal y en las relaciones del grupo en general, en caso de que los hechos hayan involucrado a compañeros o hayan ocurrido en presencia de otros estudiantes o del grupo en pleno.

Las respuestas a estos interrogantes además permitirán al docente identificar con mayor precisión si se trata de cibersituaciones Tipo I o Tipo II. Adicionalmente se sugiere,

a. Facilitar reflexión sobre la pertinencia de utilizar medios digitales como estrategia para dirimir conflictos, teniendo en cuenta posibles consecuencias y riesgos asociados.
b. Reconocer desde la perspectiva de cada uno de los estudiantes la solución reparadora.
c. Concertar las maneras concretas para reparar relaciones y efectos negativos del conflicto. En este punto, es importante que el docente formule preguntas que les permitan identificar sí la solución propuesta tiene relación directa con el hecho, si facilita que quien agrede se haga responsable de sus decisiones, sí permite superar el conflicto, sí es justa –tanto para quien agrede como para quien ha sido agredido-, y sí es viable de ser cumplida.
d. Definir cronograma para realización de los acuerdos, incluido el cronograma de la reunión de seguimiento.

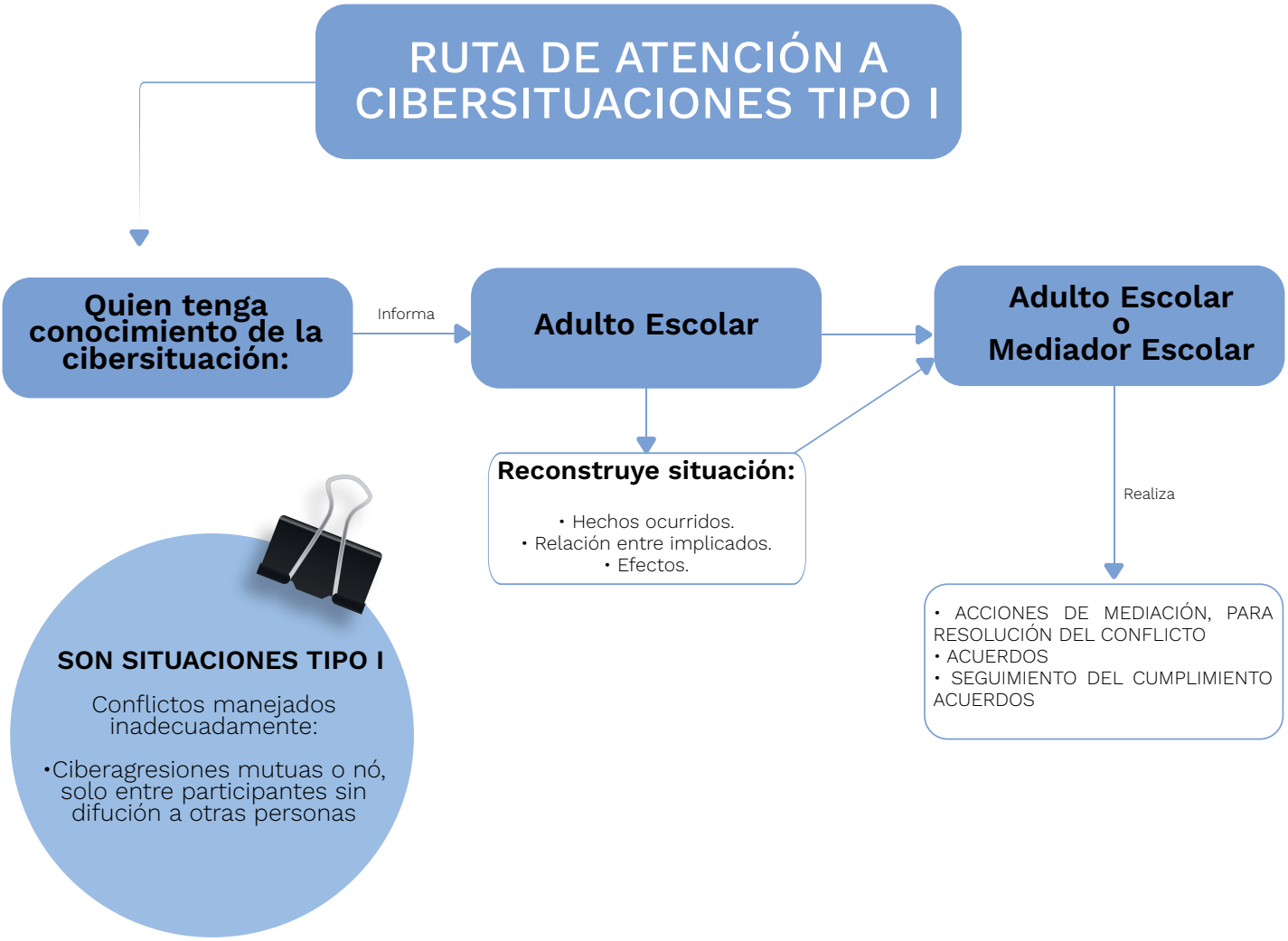
Del seguimiento de los acuerdos

a. Registrar la información obtenida por docente o estudiante mediador, en los formatos institucionalmente determinados, de manera clara y precisa, no anecdótica, para usarla como insumo sobre el proceso y elemento para realizar seguimiento. Éste debe ser firmado por los involucrados. En la medida de lo posible, cada uno deberá quedar con una copia de lo acordado.
b. Realizar seguimiento a los acuerdos establecidos. Se tomará como referente el registro de la mediación. Se realizará a través de una reunión entre docente y estudiantes involucrados en el horario y fecha previamente acordados.

Del manejo de la información

a. Desde el inicio del proceso, incluyendo la conversación con la persona que informa sobre la situación de ciberconflicto, se debe recomendar a todos, no difundir entre pares escolares información sobre la situación, en aras de no agravarla, involucrando a más personas.
b. Al mediar o arbitrar una situación de ciberconflicto entre pares escolares, evitar juicios de valor sobre los involucrados o las acciones ocurridas.
c. Acordar eliminar de dispositivos y cuentas personales las agresiones expuestas, a fin de evitar revivir la molestia o posterior uso inadecuado de éstas.

Figura 6. Ruta de atención a cibersituaciones Tipo I.



De acuerdo con el Artículo 42 del Decreto 1965, frente a las situaciones digitales Tipo I no hay en primera instancia intervención por parte de los Directivos institucionales o Directivos docentes, tampoco del Comité de Convivencia o de las familias.

4.3 Atención a situaciones digitales Tipo II.

Las situaciones que alteran la convivencia y ciberconvivencia escolar de Tipo II, son constitutivas de situaciones de acoso escolar o del uso riesgoso de las TIC que pueden causar o causan daños a la salud mental de los estudiantes involucrados, por tanto, su detección y manejo, involucra, además de la comunidad educativa, a otros actores del Sistema Nacional de Convivencia Escolar que hacen parte del grupo de instituciones garantes de los derechos de NNAJ. Particularmente, en atención a tales daños se requiere del apoyo de instituciones de salud, para poner en marcha soluciones reparadoras que restituyan los derechos vulnerados.

También en el ciberacoso, además de estudiantes directamente involucrados como agredidos y agresores, generalmente se incluyen un alto número de pares escolares u otros observadores, quienes han recibido y probablemente contribuido con la difusión de la información a través de la cual se manifiesta dicho ciberacoso. De igual manera, en las prácticas de riesgo tales como el sexting y otras señaladas como situaciones Tipo II, la audiencia puede variar entre uno o múltiples contactos.

Para que la atención a las cibersituaciones Tipo II sea oportuna y adecuada, y, apegada al debido proceso (Artículo 29 Constitución Política Colombiana; Artículos 29-30-31, Ley 1620 de 2013), se proyectan momentos diferenciados, dados de manera secuencial, a fin de que en cada uno de ellos produzcan resultados concretos que a la vez serán insumos de base para los momentos subsiguientes, todos permeados de acciones de cuidado, respeto y protección de estudiantes y personas involucradas. Entre estos se distinguen: Reconocimiento, Identificación y Activación.

El Reconocimiento, corresponde a la caracterización de qué ocurrió, envío de mensaje, meme, imagen u otro; a través de qué dispositivos, redes o plataformas; quiénes fueron participantes como agresores, agredidos y observadores; inicio de la situación; antecedentes de la misma, conflictos o acoso cara a cara previos; efectos en la salud física o mental de las personas involucradas, es decir toda la información que permita comprender plenamente lo ocurrido, y desde las miradas y perspectivas de las personas participantes.

Dependiendo de los recursos del EE se designarán personas responsables de la caracterización de los hechos. Si el EE cuenta con la presencia de Docente Orientador al momento de identificar la situación, esta sería la persona más idónea para realizar dicha caracterización. Con todo, ha de tenerse en cuenta que, si la situación ha sido informada por el estudiante agredido a su docente de mayor confianza, esta será la persona más conveniente para gestionar la caracterización a fin de brindarle la seguridad y confianza que el momento exige. De todas maneras, el proceso de caracterización de la situación se realizará siguiendo los principios de empatía y asertividad propios de la mediación a fin de que estudiantes involucrados perciban que cuentan con el apoyo institucional requerido.

De gran relevancia señalar que el EE recoge información sobre las situaciones y sus involucrados, con propósito comprensivo y de activación de rutas, no con el fin de que se constituyan en elementos probatorios con carácter judicial, lo cual sería, en caso necesario, competencia de instituciones de esa índole.

La Identificación, procede una vez caracterizada la cibersituación, y en ella el docente establece si ésta corresponde al Tipo II, y con base en ello, activa la ruta para atender y reparar los daños causados tanto a estudiantes que han sido agredidos como a sus agresores, y a mediano y largo plazo restaurar las relaciones entre dichos escolares afectando positivamente la convivencia y la ciberconvivencia escolar.

La activación se refiere a poner en marcha los protocolos con los que se cuenta en el EE, que deben haber sido previamente precisados. En todo caso, al comprobar que se trata de una cibersituación Tipo II, tal como se estipula en la Ley 1620, Artículo 21 de 2013, el docente o Docente Orientador, notificará al Comité Escolar de Convivencia, a través de contacto con su representante, sea rectoría, o coordinación de convivencia, o docente orientador -según los recursos con que cuenta el EE-. Entre el representante del Comité y dicho docente coordinarán la citación a los demás estudiantes directamente implicados –para los casos de ciberacoso-, y a las familias.

En los casos de ciberacoso, la Activación de la Ruta iniciará con la conversación con estudiantes implicados, para reconstruir los hechos desde su versión. Tomando como referencia esta información se determina la agenda y fecha de citación de las correspondientes familias. En los casos de prácticas de riesgo, también a partir del análisis logrado con la caracterización, se define la agenda para citar a las familias. De la conversación con las familias, se procede a la derivación a las Instituciones competentes. De todas las acciones realizadas, el docente o la persona encargada por el EE, realizará el registro de la situación: caracterización, agendas y fechas de citación, acuerdos y, fecha de seguimiento a los acuerdos.

4.3.1. Pasos para la activación de la Ruta de Atención de las situaciones digitales Tipo II

La información sobre situaciones de ciberacoso y de prácticas de riesgo a través de las TIC pueden ser en principio dada al docente con quien estudiantes o familia tienen mayor confianza y cercanía, o a las directivas institucionales que consideren relevantes. Quien recibe dicha información, dará trámite al proceso, tal como se estipula en la Ley 1620, Artículo 21 de 2013, lo cual incluye:

1. Reconstrucción de los hechos con estudiantes implicados, mediante conversaciones por separado con las partes. En el ciberacoso, la persona que ha sido agredida puede experimentar diversas emociones frente a quien lo agredió, entre ellas el temor, y esto lo pone en situación adicional de vulnerabilidad que dificulta lograr su versión de los hechos. No se recomienda ningún tipo de confrontación entre involucrados. Y en lo referente a prácticas de riesgo del uso de las TIC, las conversaciones separadas tienen como fin preservar la integridad e intimidad de estudiante implicado en éstas.

Sí quien informa es un familiar de estudiantes implicados u otro adulto del EE, se escucha su versión y se procede a establecer contacto con estudiantes. Para todas las conversaciones, se debe propiciar espacio seguro e íntimo en que la persona se pueda expresar con tranquilidad sin temor a ser escuchada por otros.

En la conversación que realiza la persona designada por el EE con los estudiantes que han sido agredidos y quienes han agredido, es preciso:

a. Reconocer la situación en términos de qué ocurrió, mensaje, llamada, correo electrónico, video, meme, imagen, audio, grabación, página web, blog, etc. Si es posible, recoger evidencias.
b. Precisar cuándo ocurrió la situación y si ha sido única o recurrente.
c. Identificar a través de qué medios, correos, audios, videos, mensajes, etc., se ha difundido la información.
d. Aclarar quiénes son las personas involucradas y el rol desempeñado, agresor, agredido u observador.
e. Determinar tipo de relación entre las personas involucradas.

Al finalizar la conversación, también es preciso con estudiantes:

a. Señalar que se procederá a recoger las versiones de todas las personas involucradas a fin de tener perspectiva completa de lo ocurrido, para poderlo comprender y tomar decisiones institucionales sobre manejo.
b. Si la información la brinda un tercero –estudiante observador de los hechos-, establecer si prefiere que su identidad se mantenga en anonimato. En caso afirmativo, al realizar acciones garantizar que su nombre siempre se omita y evitar cualquier tipo de riesgo físico, relacional o digital, por aportar la información.
c. Sugerir no contactar ni confrontar directamente a agresores ni a sus familias.
d. Sugerir a estudiante agredido, evitar exponerse a la red, plataforma o medio a través del que se dio la ciberagresión; y bloquear al contacto de quien provino la ciberagresión, en caso de que conozca su identidad.
e. Indicar a estudiante agredido la adopción de otras medidas de seguridad personal, no responder las provocaciones que puedan seguirse dando, utilizar las opciones de seguridad en sus redes y dispositivos, seleccionar contactos de confianza, revisar opciones para bajar la información circulante y/o detener la continuidad de su difusión y, conservar toda evidencia de la situación.
f. Recomendar que se evite comentar la situación con otras personas ajenas a ello, protegiendo la intimidad propia y la de otras personas implicadas.
g. Informar sobre el curso de acción posterior a la recolección y análisis de información: notificación y citación a familias, activación de las rutas de atención en salud, Comisaría o ICBF según corresponda, el sentido de las acciones, los tiempos probables, y, sobre la persona delegada en el EE para dar continuidad al proceso.

Si a partir de la caracterización de la situación, se observa al estudiante que ha sido agredido en estado emocional muy alterado y el EE cuenta con Docente Orientador o Docente de Apoyo, se procederá a brindarle primeros auxilios psicológicos.

Se realizará de manera inmediata una citación de las familias y la remisión al servicio de salud.

2. Notificar al Comité de Convivencia; citar a las familias de involucrados para informar de la situación, continuar su caracterización y determinar cuáles son las instituciones más competentes para contribuir a la reparación de los daños causados y la restitución de derechos de acuerdo con el grado de afectación causado.

La caracterización de la situación debe remitirse directamente al Comité de Convivencia. La información debe estar igualmente consignada en el SIUCE, y tanto dichos documentos como la información contenida deben ser mantenidos en reserva, siendo solamente usados por las personas a quienes les compete el acceso y el manejo de tal información (Ley 1581 de 2012), y como insumo documental sobre el suceso, acciones y resultados de estas.

Dependiendo de los acuerdos y organizaciones propias de cada EE, la persona encargada convocará por separado a las familias de estudiantes agredidos, agresores, y a las familias de estudiantes receptores y re-transmisores o participantes posteriores de la ciberagresión, con el fin de informar respecto a la situación y, al involucramiento y rol de su estudiante familiar en ella. Así mismo informará respecto al procedimiento efectuado, sobre continuidad del proceso acorde con directrices institucionales, y sobre rol de la familia en estas acciones posteriores.

Esta reunión puede iniciarse solo con las familias o involucrando desde su inicio al estudiante para que sea quien informe a su propia familia de lo ocurrido, de manera que proporcione su versión de los hechos, en aras de potenciar su sentido de agencia personal. No obstante, si se opta por esta forma de todas maneras se recomienda que posterior a ello haya un espacio exclusivo institución-adultos familiares, en el que puedan darse reflexiones y sugerencias de acciones por parte de estos. La decisión respecto a si se involucra o no a estudiantes en este espacio debe estar supeditada al conocimiento que se tenga sobre el tipo de relación paterno-filial existente y, sobre la preferencia de estudiantes que han sido agredidos, agresores y demás participantes. Ello porque de ninguna manera el espacio puede tornarse en enjuiciamiento colectivo, ni en elemento adicional a relaciones disfuncionales y agresivas familias-estudiantes.

Con estas consideraciones previas se sugiere en el dialogo con todas las familias, seguir las siguientes pautas:

a. Gestar un espacio cómodo, tranquilo e íntimo en el que pueda darse la información y las expresiones a que haya lugar, sin interferencias ni posibilidad de ser escuchado por otras personas.
b. Adoptar actitud empática, no inculpatoria, que facilite la comprensión de lo ocurrido por parte de las familias y así mismo, su vinculación al proceso en marcha, desde acciones puntuales que sean acordadas.
c. Informar de forma concreta, concisa, descriptiva, la situación en la que está involucrado su familiar, precisando el **Rol asumido** y así mismo **qué** ocurrió, un ciberacoso a través de mensaje, llamada, correo electrónico, video, meme, imagen, audio, grabación, página web, blog, etc. **Cuando** ocurrió en caso de ser evento único, o cuándo fue su inicio.

A través de **qué medios**, correos, audios, videos, mensajes, etc. Y, en caso de haber otras personas involucradas, **quiénes fueron**, solo omitiendo información de quien haya solicitado mantenerse en anonimato.

d. Facilitar la expresión del punto de vista familiar sobre lo ocurrido y, de posible información adicional que tengan sobre ello.

e. Indagar sobre información de antecedentes de conflicto o acoso entre estudiantes involucrados y el manejo que se ha dado.

f. Solicitar información sobre hábitos familiares digitales e involucramiento parental en vida digital de estudiantes, para identificar riesgos y protectores familiares que puedan ser usados en acciones siguientes.

g. Informar sobre las acciones que se han llevado a cabo desde el momento de recepción inicial de la información sobre la situación.

h. Sugerir asumir con su familiar, actitud de escucha, de comprensión, de rechazo hacia la ciberagresión ocurrida, de reflexión sobre daños producidos a persona agredida, y de acompañamiento para restauración y no repetición.

i. Indicar a familias no quitar dispositivos electrónicos ni prohibir acceso a internet y redes, dado su efecto negativo sobre estudiantes al impulsarlos a mantener su uso a escondidas.

j. Indicar no contactar a familias ni a demás personas involucradas, buscando no correr riesgo de agravar las situaciones por manejos impropios; ni difundir la información con otras personas, a fin de salvaguardar el derecho a la intimidad de personas implicadas.

k. Indicar los pasos posteriores que están institucionalmente establecidos: construcción colectiva del suceso; determinación de consecuencias pedagógicas y con fines restaurativos para todos los involucrados y, activación de la RUTA con las instituciones competentes y el resto de las medidas a que haya lugar de acuerdo con el Manual de Convivencia; comentar sobre el sentido de cada acción y así mismo, informar sobre las personas responsables y los posibles tiempos de ejecución.

Es imprescindible dejar constancia de la reunión, participantes, acuerdos y demás, en los formatos del registro único de situaciones de convivencia escolar, de manera clara, precisa, para que sirva como insumo del proceso, acciones y resultados y, para hacer seguimiento posterior

Una vez informadas las familias correspondientes e identificado que el daño causado no ha tenido efectos negativos en la salud mental de los estudiantes implicados, las acciones de atención vuelven sobre participantes. Quien esté institucionalmente a cargo del proceso, consultará con la persona agredida si está dispuesta y en condición emocional para llevar a cabo reunión con fines de reconstrucción colectiva de la situación de ciberacoso ocurrida y determinación de medidas de reparación y no repetición.

Se organiza dicho espacio, con la inclusión o no de la persona afectada, cuya pretensión es el reconocimiento colectivo de la situación mediante una puesta en común que permita determinar y reflexionar sobre la participación personal desde diversos roles, factores motivacionales personales y grupales que impulsaron a la vinculación en la situación de ciberagresión, posibles factores de riesgo que lo permitieron, creencias normativas sobre agresión y violencia, posibles presiones o normas grupales al respecto, y muy importante sobre el daño causado a estudiante afectado o afectada. Desde estas reflexiones se procede con los acuerdos individuales y colectivos para reparar en la víctima el daño producido, teniendo en cuenta su aceptación de lo propuesto, en tanto lo considere apropiado y proporcional a su afectación por la situación.

Para dicha reunión se sugiere:

a. Propiciar ambiente y lugar con suficiente comodidad y privacidad para que estudiantes tengan tranquilidad de expresarse con libertad, sin interrupciones ni posibilidad de ser escuchados por personas ajenas a la situación.
b. Presentar los temas a abordar y sus objetivos concretos.
c. Definir acuerdos de cómo se manejará la reunión en torno a la comunicación: escuchar a quien está hablando, solicitar la palabra sin interrumpir, evitar calificativos hacia las personas, referirse a los hechos, excluir todo tipo de agresión verbal o gestual, hacer los comentarios para todos los participantes, etc., y, todos aquellos otros que el grupo estime convenientes dadas sus características y dinámicas.
d. Dar la posibilidad a estudiantes de proponer las estrategias para promover la discusión grupal, la reflexión individual, socialización u otras, usando escritura en blog, wiki, grupos en plataforma, entre otros, a fin de promover el uso adecuado de sus competencias digitales y su capacidad para resolver situaciones negativas de ciberconvivencia en las que están involucrados.
e. Enfatizar durante el dialogo colectivo, lo inaceptable del ciberacoso, la responsabilidad moral con los efectos sobre persona agredida, las implicaciones personales de involucrarse en estas situaciones y, las necesidades personales y grupales para fortalecerse frente a riesgos posteriores de ciberagresión.
f. Desarrollar la reunión de acuerdo con lo antes pactado, precisando información sobre: qué, cuándo, de que maneras, quienes, y dónde ocurrieron las ciberagresiones; análisis, de motivos personales y grupales, de posturas frente al ciberacoso, reconocimiento de los efectos negativos en la persona agredida y sobre ellos mismos; determinación de medidas de reparación para persona afectada y de fortalecimiento personal y grupal para evitar repetición.
g. Establecer momentos y personas responsables de hacer seguimiento para verificar cumplimiento de acuerdos entre involucrados.
h. Sugerir firma de acta con acuerdos, gestionada por los propios estudiantes involucrados.
i. Consignar lo ocurrido en la reunión, en formatos institucionales establecidos para este propósito.

Este momento es pues una práctica restaurativa, que pretende reconstruir relaciones afectadas por las situaciones ocurridas, aprender de ellas para no incurrir nuevamente en situaciones similares, y, fortalecer aquello que facilitó la ciberagresión. Se torna así en un insumo esencial para proyectar acciones posteriores desde el Comité de Convivencia de manera que, los riesgos conducentes a estas situaciones puedan ser prevenidos con la comunidad educativa y especialmente con los grupos involucrados.

3. Remitir a las instituciones garantes con competencia en las situaciones. Las afectaciones emocionales son competencia del sector salud; los problemas de familia son competencia de ICBF o de la Comisaría de Familia. Cuando en un municipio o vereda no hay habilitados servicios de salud mental -psicología o psiquiatría-, la Comisaría apoya la remisión a salud. Así mismo, cuando se observa negligencia o problemas familiares de fondo, como parte de las causas de la situación que está atravesando el estudiante, el ICBF es la institución competente, sin embargo, en los municipios donde no hay cobertura, sus funciones las asume Comisaría de Familia.

Una vez caracterizada la situación, e identificado que el estudiante agredido está afectado negativamente en su salud emocional; o que el estudiante agresor y los observadores que conminaron con la ciberagresión están en situación de riesgo en su salud mental, y, luego de haber citado a las familias, estas remisiones son realizadas por el Docente Orientador o, en su defecto, se orienta a las familias para que realicen las consultas pertinentes con dichas instituciones.

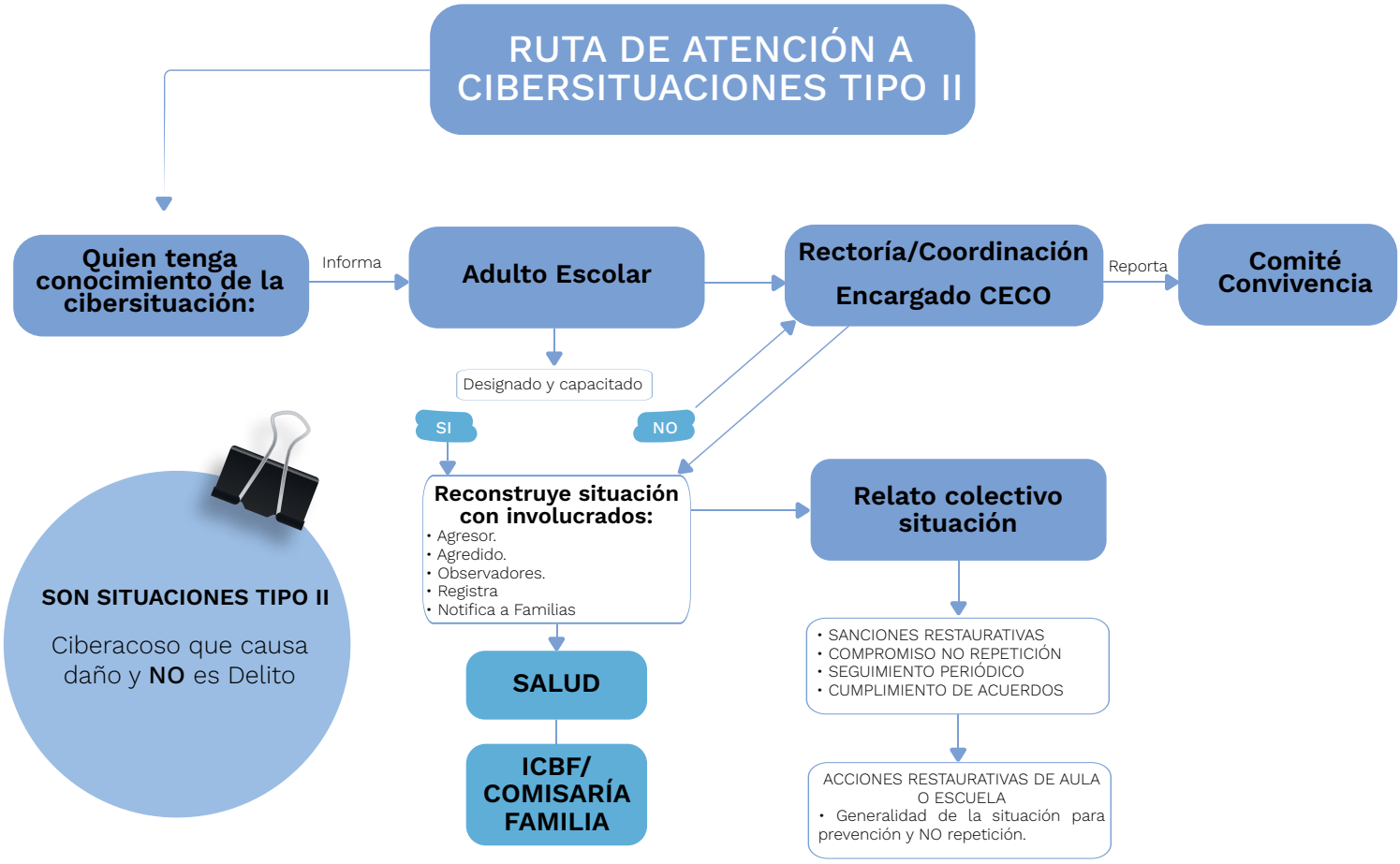
Sí adicionalmente en la caracterización de los hechos, tanto en las conversaciones individuales y colectivas con estudiantes o en las conversaciones con las familias, se observa un estado de abandono emocional hacia los estudiantes, el Comité de Convivencia en cabeza del Docente Orientador o a quién hayan delegado, realiza la respectiva remisión a ICBF o Comisaría de Familia. Esto siempre con el ánimo de promover una mejora en la convivencia familiar y en la garantía del desarrollo integral del estudiante.

Para los casos de prácticas de riesgo, luego de haber citado a las familias e identificado qué nivel de involucramiento tiene el estudiante con las prácticas de uso de las TIC, se sugiere y sí es necesario, realizar remisión a las instituciones con competencia, de acuerdo con lo estipulado anteriormente.

Todo el proceso de la cibersituación Tipo II será registrado en el formato único de registro de situaciones de convivencia escolar.

El presidente del Comité de Convivencia en reunión formal informará a los restantes miembros del mismo sobre lo ocurrido, las acciones llevadas a cabo y las medidas adoptadas, para que se proceda con el análisis del suceso y el seguimiento a lo que se haya acordado, verificando especialmente que ello redunde en beneficio de la persona afectada, en favor de la convivencia escolar y en el manejo responsable de medios digitales por parte del estudiantado. Cumpliendo con lo establecido, también habrá constancia de esta reunión de parte del Comité. Así mismo, notificará la situación al Comité Municipal de Convivencia Escolar.

Figura 7. Ruta de atención a cibersituaciones Tipo II.



4.4. Acciones para la atención a situaciones digitales Tipo III.

Se enmarcan en esta clasificación, las cibersituaciones entre estudiantes o aquellas en las que sean afectados, que sean consideradas delictivas, presuntamente atentando contra la libertad, la integridad y la formación sexual (Título IV del Libro 11 de la Ley 599 de 2000), u otras tipificadas como delito según el Código Penal Colombiano vigente (Decreto 1965 de 2013, artículo 40). Se reconocen como tales, al ser además violatorias de derechos a la intimidad, la honra y el buen nombre y, que sean realizadas a través de las Tics, conocidas también como ciberdelitos, delitos digitales o delitos tecnológicos.

Tal como se ha mencionado, entre los posibles delitos informáticos que pueden ocurrir entre pares escolares o ser identificados desde la cotidianidad escolar, se destacan: las ciberamenazas, la coacción o chantaje, la extorsión, la pornografía infantil, la suplantación de identidad, la calumnia e injuria, la circulación de mensajes o imágenes personales, íntimas y con contenidos eróticos surgidos al interior de una relación entre pares, la incitación a acciones violentas contra sí mismo o contra otros, el sonsacamiento con fines sexuales de adultos hacia menores, entre otras.

Es imprescindible recordar que la atención a las cibersituaciones Tipo III, que constituyen delitos presuntamente cometidos por estudiantes o que, en su defecto, los estudiantes sean víctimas, implica la participación del sector salud, el sistema de Responsabilidad Penal Adolescente (SRPA) y el Sistema Judicial. En estas situaciones, el rol de la comunidad educativa –docentes y directivos- principalmente versa sobre: recibir la información e iniciar el registro en el SIUCE, citar a las familias para notificar sobre los hechos y/o brindarles acompañamiento para que las éstas activen las rutas. En el caso en que la familia no active las rutas de manera oportuna para proteger la integridad de sus hijos o menores de edad a su cargo, la IE, en cabeza del Comité procederá a notificar a ICBF o la Comisaría de Familia sobre la situación. De igual manera, el CECO informará al respectivo Comité Municipal de Convivencia Escolar.

A partir de la información preliminar allegada, que permite intuir la participación de un estudiante como presunto actor o como víctima de una ciberagresión configurada como delito según normativa nacional vigente, las acciones iniciales en el EE –en cabeza de la rectoría- se enfocan entonces promover la pronta atención para garantizar la restitución de los derechos vulnerados, incluidos el derecho a la salud mental y física, toda vez que los hechos desencadenen en los estudiantes involucrados afecciones psicológicas o somáticas. En este proceso, la notificación y citación a las familias es inmediata y de carácter urgente, así como la remisión de servicio de salud, en los casos que se requiriera.

De acuerdo a la Ley 1620 de 2013, en la atención institucional a cibersituaciones Tipo III, solamente intervienen las instancias y miembros de comunidad educativa mencionados, Directivo Institucional o membros delegados del Comité de Convivencia, Comité de Convivencia, estudiantes involucrados y sus familias.

En cuanto al ingreso a los procesos y procedimientos del SRPA, éste tendría lugar por parte del EE toda vez, que las familias actúen de manera negligente o que el presunto agresor haga parte de los adultos de la comunidad educativa. En este sentido, el adulto escolar designado, actúa de acuerdo con lo establecido (numeral 3, Artículo 44; Artículo 45 Decreto 1965, 2013), a la entidad correspondiente. Dicha obligatoriedad de reporte vale recordar, está establecida en la Constitución Política Colombiana como “deber ciudadano” que contribuye con la adecuada administración de justicia (Artículo 95 Constitución Política Colombiana, 1991; Artículo 67 de la Ley 906, 2004); por tanto dicho reporte no es optativo o discrecional de cada EE y, ello conlleva adicionalmente la responsabilidad de contar con información clara y actualizada de normativas y jurisprudencia que tengan relación directa con presuntos delitos que conforman este tipo III de cibersituaciones con escolares.

En caso contrario, y frente a la duda sobre si una cibersituación entre estudiantes se configura como delito, lo pertinente es elevar consulta a dichas instancias, o a la Defensoría de Familia, Defensoría del Pueblo, Comisaría de Familia, Personería Municipal, a las Oficinas Jurídicas de las Secretaría de Educación certificadas, o a cualquier otra entidad que a nivel territorial sea parte integrante del Comité Territorial de Convivencia Escolar.

No obstante, es preciso destacar que, ante la posibilidad de un ciberdelito entre estudiantes o en el que resulten afectados, no es el EE quien tipifica las acciones a partir de la recolección de elementos materiales probatorios para un peritazgo fiscal, una vez que dicho proceso está más allá de su competencia.

Al EE le corresponde el reconocimiento de la situación y los actores involucrados, a través de sus versiones, para con ello poner en marcha las acciones reglamentadas tanto por Ley 1620 y el Decreto 1965 (2013), como por las normativas anteriormente destacadas. Sin embargo, aunque el manejo por parte de las entidades de salud, protección y justicia involucradas es propio de cada una de ellas, paralelamente el EE lleva a cabo acciones pedagógicas colectivas con estudiantes para dar cumplimiento a su compromiso misional de educar para la vida, asumiendo tales situaciones, como se ha venido señalando, como oportunidades para retroalimentar las acciones institucionalmente realizadas en aras del fortalecimiento de la convivencia y la ciberconvivencia.

No obstante, es preciso destacar que, ante la posibilidad de un ciberdelito entre estudiantes o en el que resulten afectados, al EE solo le corresponde el reconocimiento de la situación a partir de escuchar la versión de quien denuncia la situación, y realizar el registro de los hechos, sin incurrir en la reconstrucción de hechos con actores involucrados. Las denuncias ante docentes y directivos, pueden llegar de parte de los mismos estudiantes afectados, sus familias u otro actor de la comunidad educativa que ha observado. Con la información entregada, la rectoría, reporta el hecho en el formato de registro de las situaciones que alteran la convivencia escolar, para con ello poner en marcha las acciones reglamentadas tanto por Ley 1620 y el Decreto 1965 (2013), como por las normativas anteriormente destacadas.

Cabe señalar que no es competencia del EE la recolección de elementos materiales probatorios, dado que esta acción solo corresponde al SRPA. Y, el manejo de las posibles situaciones de delitos informáticos escolares es competencia de las entidades de salud, protección y justicia. Y cada una de éstas, activará su propio protocolo para la atención a estas cibersituaciones.

Con todo, paralelamente el EE lleva a cabo acciones pedagógicas colectivas con estudiantes para dar cumplimiento a su compromiso misional de educar para la vida, asumiendo tales situaciones, como se ha venido señalando, como oportunidades para retroalimentar las acciones institucionalmente realizadas en aras del fortalecimiento de la convivencia y la ciberconvivencia.

Las condiciones para la realización de estas acciones iniciales con estudiantes involucrados y las posteriores con ellos mismos o con el resto de la comunidad educativa, con fines promocionales y preventivos, son las mismas establecidas para todo el proceso de atención: empatía, carencia de enjuiciamiento, respeto, cuidado, protección a la integridad e intimidad, confidencialidad, oportunidad educativa, restauración de relaciones, reparación, entre otras.

Para lograr un adecuado manejo de posibles delitos informáticos que tengan lugar entre pares escolares o que afecten a los escolares, se proponen las siguientes recomendaciones,

4.4.1. Para los Directivos Institucionales y Comité de Convivencia

a. Contar con protocolos institucionales para atención a cibersituaciones Tipo III que afectan la convivencia y la ciberconvivencia.
b. Verificar que el protocolo de atención a cibersituaciones Tipo III, incluya formas adecuadas de registro de la información sobre procesos llevados a cabo.
c. Determinar con precisión las personas del EE implicadas en el manejo de cibersituaciones Tipo III.

d. Constatar que los adultos institucionales a cargo cuenten con las competencias personales, socioemocionales y el conocimiento óptimo para el manejo de cibersituaciones Tipo III.
e. Acordar que el manejo de la información sobre las cibersituaciones III, sea objeto de condiciones de confidencialidad y uso solo para fines específicos relacionados con procesos de convivencia y ciberconvivencia, de cara a proteger la intimidad y la integridad de estudiantes involucrados y sus familias.
f. Incluir en el Manual de Convivencia, los lineamientos para el manejo institucional a este tipo de cibersituaciones.
g. Analizar cibersituaciones Tipo III abordadas para obtener insumos sobre riesgos y protectores a incluir en acciones de promoción y prevención con comunidad educativa.
h. Informar a Orientadores y Docentes sobre cibersituaciones tipo III ocurridas (sin aludir a las personas involucradas), para que estas sean objeto de análisis y de fortalecimiento de protectores, en sus actividades con comunidad educativa.
i. Elaborar directorio de instituciones de salud, protección y justicia implicadas en manejo de cibersituaciones Tipo III que operen en la región.
j. Generar mecanismos de comunicación del protocolo de atención institucional a cibersituaciones tipo III.
k. Tramitar las cibersituaciones Tipo III, con estudiantes involucrados, familias e instituciones externas correspondientes.
l. Realizar seguimiento a acciones institucionales realizadas, verificando ante todo no repetición de ciberagresión entre implicados.

4.4.2. Para el reconocimiento de la situación

Dado el presunto carácter delictivo de la cibersituación ocurrida, el EE solo obtiene la información básica necesaria para aclarar lo ocurrido y estudiantes participantes en ello, a fin de realizar las acciones pertinentes otorgando atención oportuna y adecuada. Como se ha señalado, serán las instancias externas correspondientes quienes realicen, desde sus competencias y sus propios protocolos de atención a este tipo de situaciones, las indagaciones exhaustivas necesarias.

La información sobre estas cibersituaciones, puede también proceder de diversas fuentes, siendo estudiantes que han sido agredidos y, otros conocedores de la situación quienes probablemente la compartan con algún adulto del EE. Recuérdese que esta información, debe ser inmediatamente comunicada a la persona del EE delegada para este fin, generalmente El Rector o Rectora o, en su defecto, el miembro del Comité de Convivencia acordado. Para esta persona se sugiere,

a. Recibir la información sobre cibersituación e involucrados, que permita comprender que lo ocurrido se configura como una presunta cibersituación delictiva.
b. Reportar la cibersituación a familias de estudiantes involucrados.
c. Reportar cibersituación a aquella entidad de justicia disponible en su municipio para tal fin.
d. Remitir a institución de salud disponible, para atención a daños sobre salud física y/o mental de estudiante que ha sido cibergredido.

e. Consignar en formatos institucionales previamente diseñados, todas las actividades realizadas para manejo de la cibersituación Tipo III.
f. Proponer momentos y formas de seguimiento de efecto de las acciones realizadas, sobre estudiantes implicados.

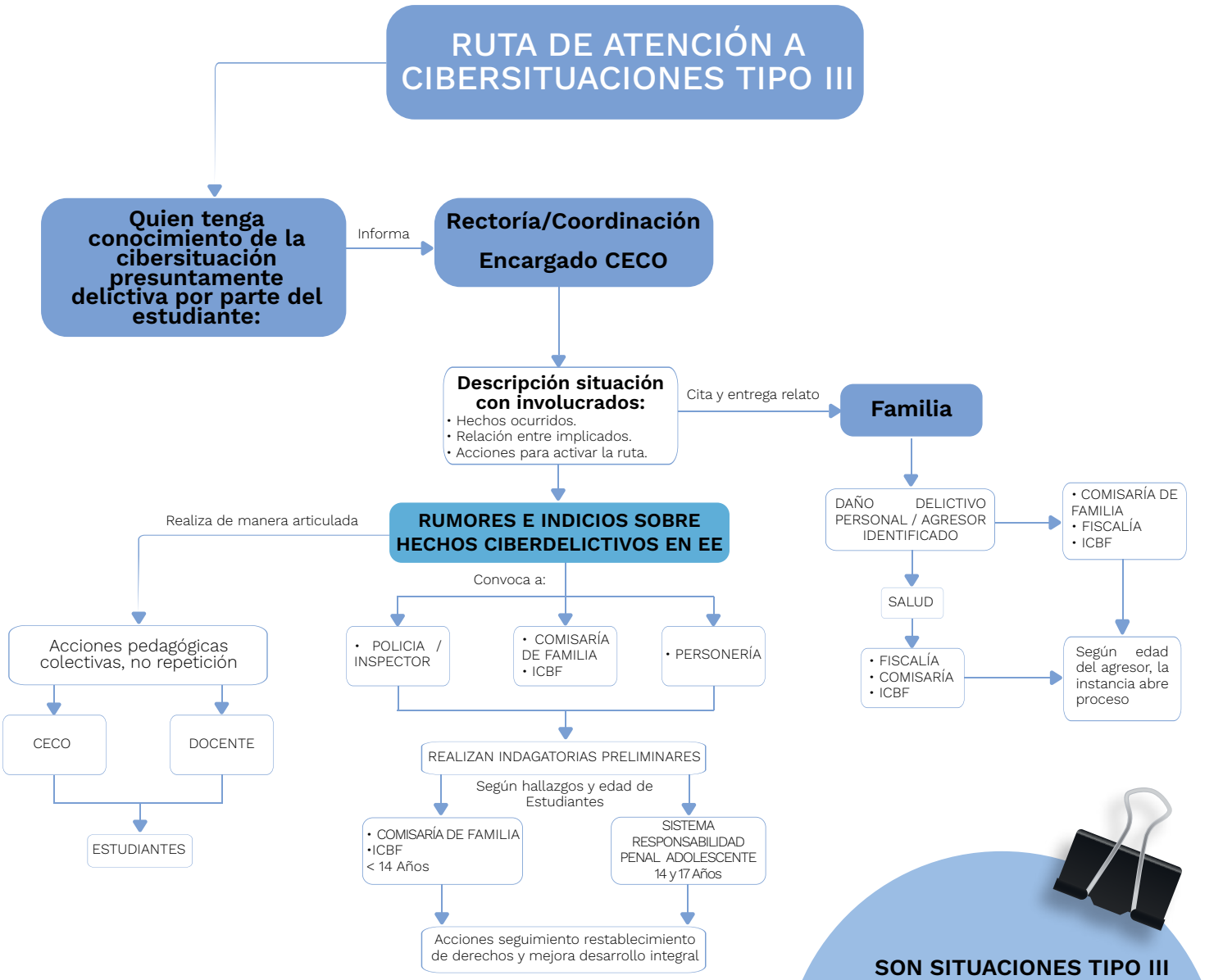
4.4.3. Con familias de implicados se recomienda,

a. Organizar un espacio propicio, privado y tranquilo, en el que se pueda dar información sobre la cibersituación ocurrida, sin interferencia ni posibilidades de ser escuchado por otras personas.
b. Informar lo ocurrido con actitud empática, evitando inculpar, de manera que se facilite comprensión por parte de las familias y su vinculación al proceso.
c. Enmarcar acciones realizadas y las subsiguientes, en normativa nacional e institucional vigente para la atención a este tipo de situaciones.
d. Informar de forma concreta, concisa, descriptiva, la situación en la que está involucrado su familiar.
e. Precisar las instancias adicionalmente involucradas en manejo de la situación a las que se remitirá el caso.
f. Facilitar la expresión del punto de vista familiar sobre lo ocurrido y, de posible información adicional que tengan sobre ello.
g. Recomendar prestar atención a efectos emocionales, de salud, relacionales, académicos y de otra índole para informarlos al EE con el propósito de darles la debida atención a los que sean de competencia institucional y, orientar acciones cuando corresponden a instituciones externas.
h. Sugerir no establecer contacto con familias de otros involucrados, evitando agravar las situaciones.
i. Solicitar no difundir la información sobre lo ocurrido con otras personas, para proteger el derecho a la intimidad de personas implicadas.
j. Dejar constancia de la reunión, en medios institucionalmente convenidos, de manera clara, precisa, para que posteriormente pueda usarse como elemento ilustrativo de procesos y acciones.

4.4.4. Con la familia de estudiante que ha sido agredido, adicionalmente,

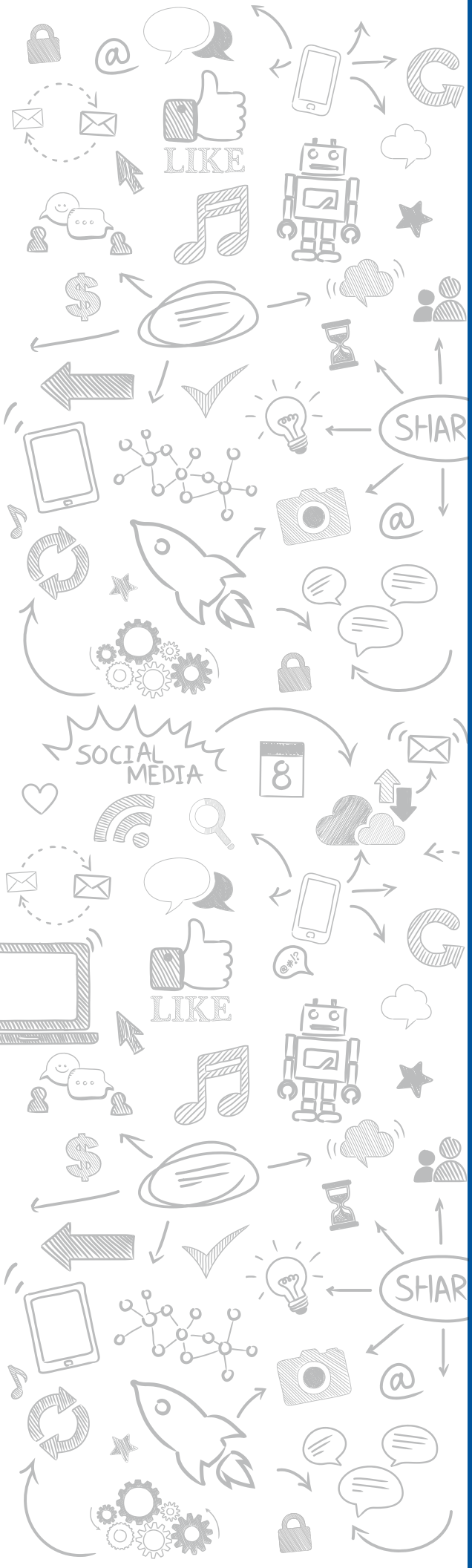
a. Sugerir acompañamiento y apoyo emocional constantes.
b. Indicar no culpabilizar por la situación ocurrida.
c. Indicar no inducir uso de agresiones reactivas y retaliación por el daño.
d. Inducir y acompañar adopción de medidas personales de ciberseguridad, bloquear al contacto del que proviene la ciberagresión; evitar responder las provocaciones en línea que puedan estarse dando; procurar no ingresar temporalmente a la red o al medio a través del que ha circulado la información agresora.
e. Sugerir adicionalmente, activar o utilizar las opciones de seguridad en sus redes y dispositivos; seleccionar contactos de confianza; revisar opciones para quitar de la red la información circulante y/o detener la continuidad de su difusión y, conservar toda la evidencia de la situación.
f. Sugerir que estudiante agredido evite contactar y confrontar directamente a agresores ni a sus familias.

Figura 8. Atención situaciones digitales Tipo III.



SON SITUACIONES TIPO III

Delitos por medios digitales, delitos contra formación sexual, injuria, calumnia, suplantación, pornografía, acoso sexual, extorisión, inducción a violencia contra sí mismo o contra otros



Del Componente de Seguimiento

5. Del componente de seguimiento.

El seguimiento, tal como lo establece el Decreto 1965 y la Guía 49 (2013), es un mecanismo con el que cuenta la RAI para llevar a cabo procesos de evaluación y monitoreo que den cuenta de planes, proyectos, acciones y sus resultados, permitiendo así un proceso vivo, dinámico, que planea, recoge, sistematiza y analiza sus experiencias, permitiendo su ajuste a las condiciones institucionales existentes. A la vez, es una fuente de comprobación de las acciones institucionales de diversa índole, proyectadas y ejecutadas para fortalecer convivencia y ciberconvivencia escolar. El seguimiento debe llevarse a cabo con todas las acciones desarrolladas en los componentes de promoción, prevención y atención a cibersituaciones Tipo I, aunque reviste especial importancia en las cibersituaciones Tipo II y III (Artículo 48 del Decreto 1965 de 2013).

Implica un proceso de evaluación, análisis y reflexión, basado en insumos concretos y preestablecidos, desde el que se determina continuidad o no de acciones, se retroalimentan elementos adicionales para fortalecer su impacto en la comunidad educativa, o se proyectan nuevas acciones. Importante también destacar la pertinencia de este componente, de cara a generar cultura institucional de evaluación para contar con datos que permitan adoptar decisiones fundamentadas sobre la ciberconvivencia, y la prevención y atención a riesgos y amenazas digitales. El proceso de seguimiento involucra tres niveles, verificación, monitoreo y retroalimentación, con los cuales se comprueba la ejecución de las acciones proyectadas, se llevan a cabo registros sistematización de las experiencias para que se constituyan en fuentes de aprendizaje institucional, y, desde estas, se cuente con insumos que nutran de manera permanente la Ruta de Atención Integral a la Convivencia Escolar.

Especial interés reviste este componente de seguimiento para la promoción de ciberconvivencia, prevención y atención del ciberacoso y delitos tecnológicos, una vez que para ello se tienen menores desarrollos nacionales que para la convivencia cara a cara, con lo cual, cada experiencia, proyecto o acción, debidamente planeado, monitoreado y evaluado en su efecto e impacto, irá construyendo y consolidando el acervo de estrategias nacionales eficaces para abordarlo, acordes con su prevalencia y características, y, adicionalmente podrán permitirle al país, ser parte de procesos evaluativos globales sobre competencias digitales del estudiantado colombiano, de cara a establecer planes a futuro.

En términos de verificación, se recomienda hacer listas de chequeo institucionales, que den cuenta si el EE desarrolló las acciones recomendadas, lo cual puede ser llevado a cabo por el Comité de Convivencia vinculando si es necesario, otros miembros de la comunidad educativa previamente designados para tal fin. Las acciones sugeridas para ser desarrolladas por Docentes, Orientadores, familias y estudiantes, deben ser elementos constitutivos de estos proyectos y acciones transversales, las maneras de llevarlos a la vida escolar cotidiana y por tanto, es imprescindible que involucren elementos evaluativos, cuantitativos o cualitativos, que permitan determinar su ejecución y sus logros.

Para el automonitoreo, primeramente es requerido precisar qué personas participarán en el proceso, también vinculando preferiblemente representantes de la comunidad educativa, en especial personas que han sido ejecutoras y beneficiarias de las acciones, para que conjuntamente construyan y /o adopten indicadores de logro y de proceso que permitan

verificar el alcance de las acciones y proyectos para ciberconvivencia ejecutados, y, si dichas acciones incidieron en las competencias digitales y socioemocionales de la comunidad educativa. Se recomienda tener en cuenta los estándares globales de DQ -inteligencia digital- (DQ Institute, 2019), que otorgan definiciones concretas de dichas competencias y sugieren cómo monitorear su logro, mostrando a la vez metas globales al respecto que pueden retroalimentar planes institucionales presentes y futuros.

Si bien al interior de cada componente y cada acción propuesta en el presente protocolo, se plantearon directrices para su seguimiento, aquí se condensan para tener una perspectiva integral de las mismas.

5.1. Seguimiento a la promoción de ciberconvivencia.

Las acciones sugeridas tienen como fin promover, facilitar y fortalecer la ciberconvivencia y la generación de ciudadanía digital en estudiantes, actuando así mismo en su entorno protector. Están enfocadas en mejorar condiciones tecnológicas y fortalecer competencias en el recurso humano, para que el EE de acuerdo con sus posibilidades y las necesidades formativas de la comunidad educativa, genere planes y proyectos en esta dirección, evalúe sus efectos e impacto en la ciberconvivencia, y dé continuidad a acciones eficaces. Se enfatiza la pertinencia de vincular en planeación y ejecución de estos planes, acciones y proyectos, a estudiantes y familias.

Tabla 11. Seguimiento a la promoción de ciberconvivencia.

VERIFICACIÓN	MONITOREO	RETROALIMENTACIÓN
• Revisar políticas institucionales para vinculación y ampliación de mejoramiento ciberconvivencia como elemento del componente de convivencia escolar. • Diseñar ajuste al Manual de Convivencia incluyendo conceptos y acciones concretas relacionadas con ciberconvivencia. • Vincular comunidad educativa en determinación necesidades en condiciones tecnológicas y de formación para ciberconvivencia y prevención y manejo riesgos tecnológicos.	• Construir indicadores que evidencien impacto de proyectos y acciones para ciberconvivencia. • Construir estrategias participativas para evaluación de proyectos y acciones. • Analizar efectividad de convocatorias a comunidad educativa para su participación en acciones proyectadas. • Determinar estrategias de convocatoria y tipo de proyectos en los que se contó con mayor vinculación de comunidad educativa	• Diseñar formas comunicativas para compartir resultados de proyectos y acciones, con comunidad educativa. • Llevar archivo de acciones comunicativas y pedagógicas sobre ciberconvinencia.

VERIFICACIÓN	MONITOREO	RETROALIMENTACIÓN
• Diseñar proyectos pedagógicos e iniciativas para fortalecer competencias digitales y ciberconvivencia escolar de acuerdo con necesidades detectadas. • Motivar presencia de estudiantes en reconocimiento necesidades y ejecución de proyectos y acciones para fortalecimiento ciberconvivencia. • Realizar acciones permanentes que permitan a comunidad educativa reconocer inclusión de ciberconvivencia como elemento importante de la convivencia escolar. • Fortalecer y mejorar de condiciones tecnológicas para su aprovechamiento como recurso de aprendizaje, comunicación y creatividad para la comunidad escolar. • Establecer incentivos para destacar proyectos y acciones que fortalezcan la ciberconvivencia. • Genera directorio de aliados estratégicos expertos en competencias digitales y ciberconvivencia. • Adoptar estrategias evaluativas globales que permitan precisar nivel de competencias para ciberconvivencia en comunidad educativa	• Reconocer impacto motivacional en la comunidad educativa, de las acciones desarrolladas. • Determinar coherencia entre PEI y plan de estudios, y, fortalecimiento y mejora de ciberconvivencia. • Identificar personas de comunidad educativa con mayor participación en acciones para ciberconvivencia. • Analizar relación entre necesidades detectadas y acciones para ciberconvivencia ejecutadas. • Reconocer efecto de acciones sobre fortalecimiento de competencias socioemocionales y digitales en comunidad educativa. • Indagar sobre efecto de acciones para ciberconvivencia en las estrategias pedagógicas de docentes.	

5.2. Seguimiento a la prevención de riesgos o amenazas digitales.

Es menester recordar que, para la prevención de riesgos digitales las acciones propuestas se focalizan en la determinación de riesgos y protectores para las amenazas digitales, de contacto, de contenidos y de comportamiento, que pueden ocurrir en el uso de las Tic. Así mismo, en el reconocimiento de aquellas de mayor incidencia o impactos más negativos en la ciberconvivencia del EE, a fin de proyectar acciones concretas que las minimicen, eviten la exposición a estas, o, en su defecto, permitan un manejo adecuado de manera tal que los impactos negativos sean menores o transitorios. Involucran igualmente a la comunidad educativa, dando continuidad a la intención enunciada desde la promoción de ciberconvivencia, de fortalecer competencias en el entorno protector de los estudiantes.

Frente a las situaciones de riesgo, se pretende reconocer las condiciones tecnológicas institucionales y, las competencias socioemocionales y digitales a fortalecer, de manera tal que actúen como protectores frente a tales amenazas.

Tabla 12. Seguimiento a la prevención de ciberacoso y delitos tecnológicos.

VERIFICACIÓN	MONITOREO	RETROALIMENTACIÓN
• Desarrollar procesos con comunidad educativa para identificar riesgos y protectores contextuales y personales frente a amenazas a la ciberconvivencia. • Establecer formas para evaluar las estrategias pedagógicas que se proyecten. • Determinar criterios para reconocimiento de estrategias pedagógicas exitosas en términos de prevención de ciberamenazas. • Diseñar protocolos de observación, registro, archivo y circulación de información sobre ciberamenazas y atenciones a las mismas. • Diseñar indicadores de logro para valorar efectos de acciones realizadas. • Realizar proceso de lectura de contexto sobre riesgos y protectores. • Construir estrategias pedagógicas con comunidad educativa para fortalecer protectores y afrontar riesgos detectados en lectura de contexto. • Acordar estrategias comunicativas sobre riesgos, protectores y acciones para prevención y manejo eficaz. • Visibilizar experiencias institucionales significativas de prevención. • Diseñar protocolos de atención a cibersituaciones Tipo I, II y III. • Concertar personas del EE que se harán cargo del manejo cibersituaciones Tipo I, II y III. • Acordar formas de registro y manejo de información de cibersituaciones Tipo I, II y III.	• Indagar por los resultados del proceso de identificación de factores de riesgo y protección. • Asignar responsabilidades y establecer formatos de registro para la evaluación de las estrategias pedagógicas acordadas. • Indagar y, posteriormente, registrar y circular información para el proceso de retroalimentación. • Diseñar indicadores de proceso sobre diseño de los protocolos. • Diseñar formatos de registro o reporte de casos atendidos con los protocolos. • Analizar si lectura del contexto facilitó identificación y priorización de factores de riesgo y protección de la comunidad educativa. • Revisar estrategias pedagógicas construidas para fortalecer protectores y minimizar riesgos digitales. • Valorar efectos de las estrategias pedagógicas sobre la prevención y manejo de ciberamenazas, en la comunidad educativa. • Determinar participación de comunidad educativa en diseño y desarrollo de estrategias de prevención acordadas. • Analizar estrategias y acuerdos para circulación y manejo de información con la comunidad educativa, sobre acciones para prevención de ciberamenazas y atención a cibersituaciones Tipo I, II y III. • Revisar si protocolos de atención a cibersituaciones Tipo I, II y III, corresponden a realidades del EE.	• Acordar estrategias de sistematización de los procesos realizados para su análisis posterior. • Diseñar espacios participativos para retroalimentación de procesos, estrategias y resultados. • Establecer formas alternativas para que la comunidad educativa pueda retroalimentar de manera constante, los procesos y acciones preventivas desarrollados. • Identificar logros y factores asociados a estos, buscando replicabilidad posterior. • Determinar estrategias y procesos no exitosos, analizando posibles factores causales. • Proponer ajustes a estrategias no exitosas, involucrando miembros de comunidad educativa beneficiarios y directamente implicados en su diseño y ejecución. • Contrastar logros de proyectos y acciones, con estándares digitales globales. • Diseñar formas para comunicar a la comunidad educativa los resultados de acciones desarrolladas para prevención de ciberamenazas.

VERIFICACIÓN	MONITOREO	RETROALIMENTACIÓN
• Establecer condición de confidencialidad con información sobre cibersituaciones Tipo I, II y III. • Incluir diferenciación de cibersituaciones Tipo I, II y III y sus manejos, en Manual de Convivencia. • Determinar instituciones o entidades externas al EE que estrarán involucradas en atenciones a cibersituaciones Tipo I, II y III. • Convenir formas de dar a conocer a comunidad educativa los protocolos de atención a cibersituaciones Tipo I, II y III y personas institucionalmente convenidas que llevarán a cabo su manejo.	• Verificar si las atenciones a cibersituaciones determinadas en los protocolos incluyen el debido proceso y son acordes con normativas vigentes. • Analizar si se cuenta con formatos de registro para hacer seguimiento de los acuerdos, acciones de reparación y demás, que se lleven a cabo durante las atenciones a las cibersituaciones Tipo I, II o III. • Verificar que instituciones o entidades externas al EE involucradas en atenciones a cibersituaciones, estén informadas de su responsabilidad en el manejo y funcionen de manera adecuada. • Revisar si protocolos de atención se vincularon a Manual de Convivencia. • Analizar si la difusión de los protocolos de atención cibersituaciones Tipo I, II y III, ha estado al alcance de la comunidad educativa.	

5.3. Seguimiento a la atención a cibersituaciones Tipo I, II y III.

Las acciones planteadas buscan que el EE cuente con estrategias concretas para proporcionar atención rápida, oportuna y eficaz, a las diversas cibersituaciones que afectan la convivencia y ciberconvivencia escolar. Al diferenciar el tipo de situaciones digitales, se pretende aumentar la eficacia institucional para su abordaje, teniendo como meta central comprender dichas situaciones de cara a cuidar, proteger y orientar, determinar acciones de reparación para quienes resultan afectados, concertar consecuencias de las propias acciones con estudiantes involucrados, pero especialmente, buscando hacer de tales situaciones experiencias de aprendizaje significativo, de cuáles factores personales, grupales u otros, facilitaron el involucramiento en ellas, para generar o fortalecer protectores que en la medida de lo posible impidan la repetición.

El EE debe constatar que estén claramente establecidos todos los protocolos de atención a las situaciones digitales, que en ellos se concreten las acciones a llevar a cabo con los miembros de la comunidad educativa implicados y así mismo, las personas institucionalmente designadas para ello. También deben incluir las formas de obtener y consignar la información sobre dichas situaciones, manteniendo las condiciones de confidencialidad y reserva. De igual forma es preciso constatar que las instituciones externas de salud, protección o justicia que puedan ser requeridas para manejos conjuntos, estén disponibles para cumplir sus funciones como actores complementarios de las atenciones pedagógicas que corresponden a los EE.

Tabla 13. Seguimiento a la atención de cibersituaciones Tipo I, II y III.

VERIFICACIÓN	MONITOREO	RETROALIMENTACIÓN
• Crear actividades que permitan reconocimiento e identificación de cibersituaciones que afectan la convivencia, la ciberconvivencia escolar y el ejercicio de los DDHH y DHSR. • Ratificar determinación de personas de comunidad educativa implicadas en el manejo de las cibersituaciones Tipo I, II y III. • Constatar en personas involucradas en atención de cibersituaciones Tipo I, II y III, formación en competencias socioemocionales y digitales necesarias para su manejo adecuado. • Ejecutar los protocolos de atención a cibersituaciones de tipos I, II, y III. • Crear conexiones con entidades e instancias externas al EE, posiblemente implicadas en manejo de situaciones Tipo II y III. • Analizar cibersituaciones Tipo II y III ocurridas en la institución, para determinar riesgos y protectores a fortalecer.	• Indagar si las actividades de reconocimiento e identificación de cibersituaciones que afectan la convivencia, la ciberconvivencia escolar y el ejercicio de los DDHH y DHSR, son pertinentes y suficientes. • Analizar el manejo dado a las cibersituaciones que afectan la convivencia y ciberconvivencia escolar, reconociendo aciertos, desaciertos, y otros elementos a incluir para su optimización. • Discutir sobre atención claramente diferenciada para cada tipo de cibersituación. • Constatar que estrategias y acciones para atención a cibersituaciones involucren enfoque de derechos para todos los participantes y sus familias. • Analizar si entidades e instituciones externas al EE vinculadas a la atención, realizan las acciones correspondientes en sus rutas. • Revisar si la comunidad educativa cuenta con la información clara y actualizada sobre las cibersituaciones y los protocolos institucionales para su manejo.	• Diseñar espacios para retroalimentar el proceso de atención a cibersituaciones, generando acciones que optimicen el proceso y se incluyan en los protocolos institucionales. • Vincular representantes de comunidad educativa, en desarrollo de propuestas para optimizar protocolos de atención a cibersituaciones que afectan la convivencia, la ciberconvivencia escolar y el ejercicio de los DDHH y DHSR.

6. BIBLIOGRAFÍA

• Bacchini, D., Esposito, G. & G. Affuso, G. (2009). Social Experience and School Bullying. Journal of Community & Applied Social Psychology, 19, 17-32.
• Baldry, A. C., Farrington, D. P., & Sorrentino, A. (2016). Cyberbullying in youth: A pattern of disruptive behaviour. Psicologia Educativa, 22(1), 19–26. http://dx.doi.org/10. 1016/j.pse.2016.02.001
• Bandura, A. (2016). Moral Disengagement. New York: Worth Publishers.
• Beckman, L., Stenbeck, M., & Hagquist, C. (2016). Disability in relation to different peervictimization groups and psychosomatic problems. Children and Schools, 38, 153–161.
• Bevilacqua, L., Shackleton, N., Hale, D., Allen, E., Bond, L., Christie, D., ... Viner, R. M. (2017). The role of family and school-level factors in bullying and cyberbullying: A cross-sectional study. BMC Pediatrics, 17(1), 160. http://dx.doi.org/10.1186/s12887-017-0907-8.
• Brewer, G., & Kerslake, J. (2015). Cyberbullying, self-esteem, empathy and loneliness. Computers in Human Behavior, 48, 255–260. http://dx.doi.org/10.1016/j.chb.2015.01.073.
• Bottino, S. B., Bottino, C. C., Regina, C. G., Correia, A. L., & Ribeiro, W. S. (2015). Cyberbullying and adolescent mental health: Systematic review. Cadernos de Saude Publica, 31(3), 463–475.
• Bronfenbrenner, U. (1981). Ecology of Human Development: Experiments by Nature and design. Cambridge: Harvard University Press
• Carvajal, B. A. (2010). Teoría y práctica de la sistematización de experiencias. Santiago de Cali: Programa Editorial Universidad del Valle. Cuarta Edición.
• Cantone, E., Piras, A. P., Vellante, M., Preti, A., Daníelsdóttir, S., D'Aloja, E., & Bhugra, D. (2015). Interventions on bullying and cyberbullying in schools: A systematic review. Clinical Practice & Epidemiology in Mental Health, 11, 58-76.
• Chen, L., Ho, S. S., & Lwin, M. O. (2016). A meta-analysis of factors predicting cyberbullying perpetration and victimization: From the social cognitive and media effects approach. New Media & Society, 19, 1194–1213. http://dx.doi.org/10.1177/
• Common Sense Media. (2020). ¿Qué es ciberbullying y cómo prevenirlo? Recuperado de https://www.commonsensemedia.org/espanol/blog/que-es-el-ciberbullying-y-como-prevenirlo
• Common Sense Media. (2020). 5 Myths and Truths About Kids' Internet Safety. Recuperado de https://www.commonsensemedia.org/blog/5-myths-and-truths-about-kids-internet-safety
• Congreso de la República (2013). Ley 1620 de 2013. Por la cual se crea el Sistema Nacional de Convivencia Escolar y formación para el ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. Recuperado de http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685356
• Congreso de la República (2013). Decreto 1965. Por el cual se reglamenta la Ley 1620 de 2013, que crea el Sistema Nacional de Convivencia Escolar y formación para el ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. Recuperado de
http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1378136
• Congreso de la República (2006). Ley 1098. Por la cual se expide el Código de la Infancia y la Adolescencia. Recuperado de https://www.icbf.gov.co/sites/default/files/codigoinfancialey1098.pdf
• Congreso de la República (2009). Ley 1273. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Recuperado de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

• Craig, W. M., & Pepler, D. J. (2007). Understanding bullying: from research to practice. Canadian Psychology, 48(2), 86-93.
• Cross, D., Lester, L. & Barnes, A. (2015). A longitudinal study of the social and emotional predictors and consequences of cyber and traditional bullying victimization. International Journal of Public Health. 60(2), 207-217
• Consejería de Educación Junta de Andalucía (2017). Instrucciones de 11 de enero de 2017 de la Dirección General de Participación y Equidad en relación con las actuaciones específicas a adoptar por los Centros educativos en la aplicación del protocolo de actuación en supuestos de acoso escolar ante situaciones de ciberacoso. Recuperado de https://www.juntadeandalucia.es/educacion/portals/abaco-portlet/content/fb2e79b3-4146-4d03-8001-9650eefc0f02
• COST IS 0801 (2013). Guidelines for preventing cyber-bullying in the school environment: a review and recommendations. Recuperado de http://sites.google.com/site/costis0801/
• Cowie, H. (2013). El impacto emocional y las consecuencias del ciberacoso. Revista digital de la asociación CONVIVES (3) 16-24.
• Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., Thomas, L., Bame, A. (2016). Longitudinal impact of the cyber friendly school program on adolescents` cyberbullying behavior. Aggressive Behavior, (42), 166-180.
• Cuevas, M. C. & Marmolejo, M. A. (2014). Observadores en situaciones de victimización por intimidación escolar: caracterización y razones de su rol. Psicología desde el Caribe, 31(1), 103-132.
• Cuevas, M. C. & Marmolejo, M. A. (2016). Observadores: un rol determinante en el acoso escolar. Pensamiento Psicológico, 14(1), 89-102 doi:10.11144/Javerianacali.PPSI14-1.orda
• Defensor del Menor en la Comunidad de Madrid (2011). Ciberbullying. Guía de recursos para centros educativos. Recuperado de http://www.madrid.org/bvirtual/BVCM013909.pdf
• Del Barrio, C. (2013). Experiencias de acoso y ciberacoso: autores, autoras, víctimas y consideraciones para la prevención. Revista digital de la asociación CONVIVES (3). 25-33.
• Del Rey, R., Lazuras, L., Casas, J. A., Barkoukis, V., Ortega-Ruiz, R., & Tsorbatzoudis, H. (2015). Does empathy predict (cyber) bullying perpetration, and how do age, genderand nationality affect this relationship? Learning and Individual Differences, 45,275–281. http://dx.doi.org/10.1016/j.lindif.2015.11.021.
• Departamento Nacional de Planeación (2019). Plan Nacional de Desarrollo 2018- 2022. Pacto por Colombia, pacto por la equidad.
• DQ Institute (2019). DQ Goblal Standars Report 2019. Common framework for digital literacy, skills and readiness. Recuperado de https://www.dqinstitute.org/dq-framework
• DQ Institute (2020). The 2020 Child on Line Safety Index Report. Recuperado de https://www.dqinstitute.org/child-online-safety-index
• Domínguez-Hernández, F., Bonell, L., & Martínez-González, A. (2018). A systematic literature review of factors that moderate bystanders' actions in cyberbullying. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 12(4), article 1.
• Elipe, P., de la Oliva Muñoz, M., & Del Rey, R. (2017). Homophobic bullying and cyberbullying: Study of a silenced problem. Journal of Homosexuality. http://dx.doi.org/10.1080/00918369.2017.1333809.
• Elsaesser, C., Russell, B., Ohannessian, C. M., & Patton, D. (2017). Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. Aggression and Violent Behavior, 35, 62–72. http://dx.doi.org/10.1016/j.avb.2017.06.004
• Espelage, D. L. (2014). Ecological Theory: Preventing youth bullying, aggression, and victimization. Theory Into Practice, 53 (4), 257-264.

• Estévez, E., Flores, E., Estévez, J., Huescar., E. (2019). Programas de intervención en acoso escolar y ciberacoso en educación secundaria con eficacia evaluada: una revisión sistemática. Revista Latinoamericana de Psicología. 51 (3), 210-225.
• Ettekal, I., Kochenderfer-Ladd, B., & Ladd, G. W. (2015). A synthesis of person and relational level factors that influence bullying and bystanding behaviors: toward an integrative framework. Aggression and Violent Behavior, 23, 75-86.
• Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. The European Journal of Developmental Psychology, 9, 168–181.
• Farrington, D. P., & Ttofi, M. M. (2011). Bullying as a predictor of offending, violence and later life outcomes. Criminal Behaviour and Mental Health, 21, 90–98.
• Finkelhor, D., Walsh, K., Jones, L., Mitchell, K. & Collier, A. (2020). Youth Internet Safety Education: Aligning programs with the evidence base. Trauma, Violence, & Abuse, sagepub.com/journals-permissions. DOI: 10.1177/152483802091625 journals.sagepub.com/home/tva
• Flores, J. (2008). Ciberbullying. Guía rápida para la prevención del acoso por medio de las nuevas tecnologías. Recuperado de http://www.ararteko.net/RecursosWeb/DOCUMENTOS/1/1_1218_3.pdf.
• Fridh, M., Lindström, M., & Rosvall, M. (2015). Subjective health complaints in adolescent victims of cyber harassment: Moderation through support from parents/friends - a Swedish population-based study. BMC Public Health, 15, 949. http://dx.doi.org/10. 1186/s12889-015-2239-7
• Garaigordobil, M. & Oñederra, J. A. (2010). La violencia entre iguales: Revisión teórica y estrategias de intervención. Madrid: Pirámide.
• Garaigordobil, M. (2011). Bullying y cyberbullying: conceptualización, prevalencia y evaluación. Facultad de Psicología. Universidad del País Vasco. Formación Continuada a distancia. Recuperado de http://www.psicologiaysexologia.org/wp-content/uploads/2013/11/Bullying-y-cyberbullyung.pdf
• Gradinger, P., Yanagida, T., Strohmeier, D., Spiel, C. (2016).Effectiveness and Sustainability of the ViSC Social Competence Program to Prevent Cyberbullying and Cyber-Victimization: Class and Individual Level Moderators. Aggressive behavior (42), 181-193.
• Herrera, M., Romera, E. & Ortega-Ruiz, R. (2018). Bullying y Cyberbullying en Latinoamérica. Un estudio bibliométrico. Revista Mexicana de Investigación Educativa, 23(76), 125-155
• Hinduja, S. (2020). Digital Citizenship in 2020 and Beyond. Recuperado de https://cyberbullying.org/digital-citizenship-research
• Hinduja, S., & Patchin, J. W. (2010). Bullying, Ciberbullying, and Suicide. Archives of Suicide Research, 14 (3), 206–221. doi:10.1080/13811118.2010.494133
• Hinduja, S. & Patchin J. W. (2012) Cyberbullying: neither an epidemic nor a rarity. European Journal of Developmental Psychology 9, 539–543.
• Hinduja, S. & Patchin, J. W. (2019). Cyberbullying warning signs red flags that a child is involved in cyberbullying. Recuperado de https://cyberbullying.org/cyberbullying-warning-signs.pdf
• Hinduja, S. & Patchin J. W. (2020). Cyberbullying: Identification, Prevention, and Response. Recuperado de https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2020.pdf
• Hyde, K. F. (2000). Recognising deductive processes in qualitative research. Qualitative Market Research. An International Journal, 3(2), 82 – 90
• Jacobs, Goossens, Dehue, Völlink, Lechner (2015), Dutch Cyberbullying Victims' Experiences, Perceptions, Attitudes and Motivations Related to (Coping with) Cyberbullying: Focus Group Interviews. Societies 5, 43-64.

• Instituto Colombiano de Bienestar Familiar (2019). Riesgos digitales, ¿Cómo proteger a niñas, niños y adolescentes cuando navegan en internet? Recuperado de https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos
• Instituto Nacional de Tecnologías de la Educación. INTECO (2012). Guía de actuación contra el ciberacoso. Recuperado de http://www.injuve.es/sites/default/files/2013/46/publicaciones/Gu%C3%ADa%20de%20actuaci%C3%B3n%20contra%20el%20ciberacoso.pdf
• Juvonen, J., & Gross, E.F. (2008). Extending the school grounds? Bullying experiences in cyberspace. The Journal of School Health, 78, 9, 496-505.
• Kenny, U., Sullivan, L., Callaghan, M., Molcho, M., & Kelly, C. (2017). The relationship between cyberbullying and friendship dynamics on adolescent body dissatisfaction: A cross-sectional study. Journal of Health Psychology1359105316684939. http://dx.doi.org/10.1177/1359105316684939.
• Kowalski, R. M., Morgan, C. A., Drake-Lavelle, K., & Allison, B. (2016). Cyberbullying among college students with disabilities. Computers in Human Behavior, 57, 416– 427. http://dx.doi.org/10.1016/j.chb.2015.12.044.
• Kowalski, R. M., Giumetti, G., Schroeder, A., & Lattanner, M. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140, 1073–1137. http://dx.doi.org/10.1037/a0035618.
• Kowalski, R. M., Toth, A., & Morgan, M. (2017). Bullying and cyberbullying in adulthood and the workplace. Journal of Social Psychology. http://dx.doi.org/10.1080/00224545.2017.1302402.
• Kowalski R, Limber S y Agatston P (2010). Cyber Bullying: El acoso escolar en la era digital. Bilbao: Desclée de Brower. (original publicado en 2008) Kowalski, R. M., Limber, S. P. & McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. Aggression and Violent Behavior 45, 20–32
• Lanzillotti, A.I., & Korman, G.P. (2020). Motivos del Maltrato Escolar y del Cyberbullying desde la Perspectiva de los Estudiantes. Estudio con Adolescentes de Buenos Aires. Revista Científica Hallazgos21, 5(1), 11-33. Recuperado de http://revistas.pucese.edu.ec/hallazgos21/
• Lee, E. B. (2017). Cyberbullying: Prevalence and predictors among African American young adults. Journal of Black Studies, 48(1), 57–73. http://dx.doi.org/10.1177/0021934716678393.
• Lee, J. M., Hong, J. S., Yoon, J., Perguero, A. A., & Seok, H. J. (2017). Correlates of adolescent cyberbullying in South Korea in multiple contexts: A review of the literature and implications for research and school practice. Deviant Behavior, 39,293–308.
• Lee, C., & Song, J. (2012). Functions of parental involvement and effects of school climate on bullying behavior among South Korean middle school students. Journal of Interpersonal Violence, 27, 2437–2464.
• Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. Computers in Human Behavior, 23, 1777-1791.
• Lianos, H., & McGrath, A. (2017). Can the general theory of crime and general strain theory explain cyberbullying perpetration? Crime & Delinquency, 1–27. http://dx.doi.org/10.1177/0011128717714204.
• Machimbarrena, J. M., González-Cabrera, J., & Garaigordobil, M. (2019). Variables familiares relacionadas con el bullying y el cyberbullying: una revisión sistemática. Pensamiento Psicológico, 2, 37–56.https://doi.org/https://doi.org/10.11144/doi:10.11144/Javerianacali.PPSI17-2.vfrb

• Martins, M. D., Veiga Simão, A. M., Freire, I., Caetano, A. P., & Matos, A. (2016). Cybervictimization cyber-aggression among Portuguese adolescents: The relation to family support and family rules. International Journal of Cyber Behavior, Psychology and Learning, 6(3), 65–78. http://dx.doi.org/10.4018/IJCBPL.2016070105.
• Martínez, M. (2008). Epistemología y Metodología Cualitativa en las Ciencias Sociales. México: Editorial Trillas.
• Marwick, A.E. & Boyd, D. (2011). The drama! Teen conflict, gossip, and bullying in networked publics. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 2011. Available at SSRN: http://ssrn.com/paper=1926349
• Migliaccio, T. & Raskauskas, J. (2015). Bullying as a Social Experience: Social factors, prevention and intervention. Burlington: Ashgate Publishing Company.
• Ministerio de Educación Nacional. (2013). Guías pedagógicas para la convivencia escolar. Bogotá: Ministerio de Educación Nacional.
• Mueller, W. (2012). A parents guide to ciberbullying. - Digital kids initiative. Recuperado de https://digitalkidsinitiative.com/wp-content/uploads/2012/01/Cyberbully_handout.pdf de
• Orpinas, P. & Horne, A, M. (2006). Bullying Prevention: Creating a positive school climate and developing social competence. Washington, DC: American Psychological Association.
• Olweus D. (2012). Cyberbullying: an overrated phenomenon? European Journal of Developmental Psychology 9, 520–538.
• Olweus, D. (2013). School bullying: Development and some important challenges. Annual Review of Clinical Psychology, 9, 1–14. http://dx.doi.org/10.1146/annurev- clinpsy-050212-185516.
• Organización de las Naciones Unidas (1989). Convención sobre los Derechos del Niño.
• Ortega-Barton, J., Buelga, S., & Cava, M. (2016). The influence of school and family environment on adolescent victims of cyberbullying. Comunicar, 24(46), 57–65.
• Ortega, R., Elipe, P., Mora-Merchán, J. A., Calmaestra, J. & Vega, E. (2009). The emotional impact on victims of traditional bullying and cyberbullying: A study of Spanish adolescents. Zeitschrift Fur Psychologie/ Journal of Psychology, 217, 197- 204.
• Ortega-Ruiz, R. (2020). Educación para el Desarrollo Sostenible : del proyecto cosmopolita a la ciberconvivencia. Investigación en la Escuela, 100, 11–22.
• Ortega-Ruiz, R., Del Rey, R. y Casas, J. A. (2013). Redes sociales y cyberbullying: El proyecto ConRed. En Revista digital de la asociación CONVIVES (3). 34-44
• Patchin, J. & Hinduja, S. (2006) Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4, 148-169.
• Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and Violent Behavior, 34, 193–200. http://dx.doi.org/10.1016/j.avb.2017.01.012.
• Prochaska, J. & DiClemente, C. (1982). Transactional therapy: toward a more integrative model of change. Psichoterapy: theory, research and practice, 19, 276-288.
• Programa de las Naciones Unidas para el Desarrollo (2015). Objetivos de Desarrollo Sostenible.
• Queensland Anti Ciberbullying Task Force (2018). Adjust our settings: A community approach to address cyberbullying among children and young people in Queensland. Recuperado de https://campaigns.premiers.qld.gov.au/antibullying/taskforce/assets/anti-cyberbullying-taskforce-final-report.pdf
• Rutter, M. (2000). Resilience reconsidered: Conceptual considerations. En Handbook of early childhood intervention (2nd ed.), pp. 651-682. New York: Cambridge University Press.
• Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49, 376-385.

• Salmivalli, C. (2010). Bullying and the peer group: a review. Aggression and Violent Behavior, 15, 112-120
• Shapka, J. D., & Law, D. M. (2013). Does One Size Fit All? Ethnic Differences in Parenting Behaviors and Motivations for Adolescent Engagement in Cyberbullying. Journal of Youth and Adolescence, 42, 723–738. https://doi.org/10.1007/s10964-013-9928-2
• Shapka, J. D., Onditi, H. Z., Collie, R. J., & Lapidot-Lefler, N. (2018). Cyberbullying and cybervictimization within a cross-cultural context: A study of Canadian and Tanzanian adolescents. Child Development, 89, 89–99.
• Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2008). "Cyberbullying: Its nature and impact in secondary school pupils." Journal of Child Psychology & Psychiatry 49, 376–385.
• Souza, S. B., Veiga Simao, A. M., Ferreira, A. I., & Costa Ferreira, P. (2017). University students' perceptions of campus climate, cyberbullying and cultural issues: Implications for theory and practice. Studies in Higher Education, 1–16. http://dx.doi.org/10.1080/03075079.2017.1307818.
• Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277-287.
• Thornberg, R. (2015). The social dynamics of school bullying: The necessary dialogue between the blind men around the elephant and the possible meeting point at the social-ecological square. Confero Essays on Education Philosophy and Politics 3(1). DOI: 10.3384/confero.2001-4562.1506245
• Thornberg, R., Pozzoli, T., Gini, G. & Hong, S. J. (2017). Bullying and repeated conventional transgressions in Swedish schools: How do gender and bullying roles affect students' conceptions? Psychology. Sch. 54, 1189–1201. doi: 10.1002/ pits.22054
• Thornberg, R., Thornberg, U. B., Alamaa, R. & Daud, N. (2016). Children's conceptions of bullying and repeated conventional transgressions: moral, conventional, structuring, and personal-choice reasoning. Educational Psychology, 36, 95–111. doi: 10.1080/01443410.2014.915929
• Thornberg, R., Wänström, L. & Hymel, S. (2019). Individual and classroom social- cognitive processes in bullying: a short-term longitudinal multilevel study. Frontiers of Psychology, 10:1752. doi: 10.3389/fpsyg.2019.01752
• Ttofi, M. M., Farrington, D. P., & Lösel, F. (2011). Editorial: Health consequences of school bullying. Journal of Aggression, Conflict and Peace Research, 3, 60–62.
• Tolsma, J., van Deurzen, I., Stark, T. H. & Veenstra, R. (2013).
• Unesco (2017). School violence and bullying. Global Status Report.
• Unesco (2019). Behind numbers: ending school violence and bullying.
• Unicef - Ministerio de Educación Pública Costa Rica (2015). Protocolo de actuación en situaciones de bullying. Recuperado de https://www.mep.go.cr/sites/default/files/protocolo-actuacion-situaciones-bullying.pdf
• Unicef- Gobierno de la provincia de Buenos Aires (2017). Guía de sensibilización sobre Convivencia Digital. Recuperado de https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf
• Unicef (2018). For every child every right. Annual Report.
• Unicef (2019). Niños, niñas y adolescentes en línea. Riesgos de las redes y herramientas para protegerse. Recuperado de https://www.unicef.org/guatemala/informes/ni%C3%B1os-ni%C3%B1as-y-adolescentes-en-l%C3%ADnea
• Unicef (2020). Ocultos a plena luz.

• Vandebosch, H., & van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. New Media and Society New Media and Society, 11(8), 1349-1371.
• Valdebenito, S., Ttofi, M., & Eisner, M. (2015). Prevalence rates of drug use among school bullies and victims: A systematic review and meta-analysis of cross-sectional studies. Aggression and Violent Behavior, 23, 137–146.
• Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. Computers in Human Behavior, 69, 268–274. http://dx.doi.org/10.1016/j.chb.2016.12.038.

ANEXO 1.

GLOSARIO DE TÉRMINOS

TÉRMINO	SIGNIFICADO
ALFABETIZACIÓN DIGITAL	Adquisición de hábitos adecuados de uso de las TIC para comprender, manejar y disfrutar de ellas.
APP	Es una aplicación que se instala en un dispositivo digital. Son de diversas categorías como Educación, Deportes, Noticias, Entretenimiento, Salud, Juegos, Fotografía, Tiempo, etc.
BLOQUEAR	Negar el acceso de otra persona para que no pueda acceder a publicaciones, chats u otras actividades en línea del usuario.
CHAT	Conversación en línea en tiempo real.
CIBERACOSO	Comportamiento agresivo, intencional y compartido a través de redes sociales, mensajería, plataformas, juegos en línea, para burlarse, ofender, humillar, hacer quedar mal, excluir, difamar a una persona que no puede defenderse fácilmente, que le produce daños a su dignidad e integridad.
CIBERCONVIVENCIA	Relaciones entre personas de comunidad virtual basadas en el respeto a derechos y deberes, para beneficio de ventajas y oportunidades digitales. Se apoya en Netiqueta, o pautas de "buenas maneras" en línea.
CIBERESPACIO	“Universo" electrónico creado por las redes informáticas en las que las personas interactúan.
CIBERSEGURIDAD	Herramientas y mecanismos para la protección de redes, dispositivos, cuentas y datos personales en el ciberespacio.
COMPETENCIAS DIGITALES	Conjunto de herramientas que den como resultado un uso creativo, crítico y seguro de las TIC para aprender, comunicarse, crear y divertirse.
CIUDADANÍA DIGITAL	Conocimientos y competencias socioemocionales y digitales, valores y actitudes para desenvolverse en la comunidad virtual de manera responsable, segura y ética, usando tecnología para aprender, crear, comunicarse y disfrutar.
DELITOS TECNOLÓGICOS O DIGITALES	Acción considerada delictiva en normativa nacional, realizada por estudiantes en espacio digital. Suele incluir injuria o calumnia, amenaza, extorsión, acoso sexual, pornografía infantil, suplantación, inducción a violencia contra sí mismo u otros, discriminación por raza, credo, identidad sexual u otro.

TÉRMINO	SIGNIFICADO
EXCLUSIÓN DIGITAL	Sacar a una persona de un chat o grupo al que pertenecía o pretende pertenecer, bloquearla para que no pueda continuar participando.
GROOMING	Adultos que intentan reclutar menores para tener encuentros sexuales en línea o fuera de línea o para obtener imágenes o videos sexuales. Generalmente adoptan perfiles falsos para acercarse a sus víctimas y ganarse su confianza.
HUELLA DIGITAL	Toda información en línea sobre una persona, que se va generando por las actividades, publicaciones y comentarios que hace en el ciberespacio, que va formando parte de su identidad digital.
INFLUENCIADOR	Persona que puede influir en una audiencia a través de una red o plataforma digital. Generalmente cuenta con muchos seguidores.
INMIGRANTE DIGITAL	Persona que no ha crecido con la tecnología digital, y la ha adoptado posteriormente por necesidad o exigencia.
INTELIGENCIA DIGITAL	Conjunto de competencias socioemocionales y digitales que permiten a los escolares beneficiarse de las oportunidades del ciberespacio para ampliar su aprendizaje, sus relaciones interpersonales, conectarse con el mundo, disfrutar de diversión en línea, crear y contar con mejores herramientas para su vida y su desarrollo laboral posterior.
MEMES	Fotos o videos subtitulados, retocados, que tienen la intención de ser divertidos, usados para ridiculizar públicamente a alguien o a algo.
NATIVO DIGITAL	Conocimientos y competencias socioemocionales y digitales, valores y actitudes para desenvolverse en la comunidad virtual de manera responsable, segura y ética, usando tecnología para aprender, crear, comunicarse y disfrutar.
NETIQUETA	Persona que ha crecido con la tecnología digital, ha sido parte de su desarrollo y tiene mucha facilidad para usarla.
PORNOVENGANZA	Distribuir en las redes, sin consentimiento, una fotografía íntima de otra persona, con fines de venganza.
PISHING	Técnica usada para obtener información personal, confidencial, generalmente mediante correos electrónicos fraudulentos.

TÉRMINO	SIGNIFICADO
RIESGOS O AMENAZAS DIGITALES	Situaciones en línea que amenazan la ciberconvivencia y la seguridad. Hay riesgos de contacto, al relacionarse con personas inapropiadas, riesgos de contenido, por ser inadecuados para edad (pornografía) o inducir a odio, violencia contra uno o contra otros, y, Riesgos de conducta, al realizar acciones de ciberacoso, compartir imágenes personales íntimas o eróticas, descuidar seguridad personal de cuentas y privacidad.
SEGUIDOR	Persona que ha solicitado a otra que le permita conectarse con sus redes sociales (Twitter, Instagram y sitios similares).
SEXTING	Envío o recepción de contenido sexualmente explícito o sugerente, erótico, de imágenes o videos a través del teléfono o Internet.
SEXTORSIÓN	Chantaje que se le hace a una persona al tener una imagen suya íntima, amenazando publicarla en la red.
TICS	Tecnologías de la Información y la Comunicación
VIRAL	Contenido que se difunde con gran rapidez y al que acceden un gran número de personas.

Adaptado de: Defensor del Menor en la Comunidad de Madrid, 2011; Hinduja y Patchin, 2020; INTECO (s.f); UNICEF, 2019.

ANEXO 2.

DECÁLOGO E-DERECHOS

1. **Derecho al acceso a la información y la tecnología,** sin discriminación por motivo de sexo, edad, recursos económicos, nacionalidad, etnia, lugar de residencia, etc. En especial este derecho al acceso se aplicará a los niños y niñas discapacitados.

2. **Derecho al esparcimiento, al ocio, a la diversión y al juego,** también mediante Internet y otras nuevas tecnologías. Derecho a que los juegos y las propuestas de ocio en Internet no contengan violencia gratuita, ni mensajes racistas, sexistas o denigrantes y respeten los derechos y la imagen de los niños y niñas y otras personas

3. **Derecho a la intimidad de las comunicaciones por medios electrónicos.** Derecho a no proporcionar datos personales por la Red, a preservar su identidad y su imagen de posibles usos ilícitos.

4. **Derecho al desarrollo personal y a la educación,** y a todas las oportunidades que las nuevas tecnologías como Internet puedan aportar para mejorar su formación. Los contenidos educativos dirigidos a niños y niñas deben ser adecuados para ellos y promover su bienestar, desarrollar sus capacidades, inculcar el respeto a losderechos humanos y al medio ambiente y prepararlos para ser ciudadanos responsables en una sociedad libre.

5. **Derecho a beneficiarse y a utilizar en su favor las nuevas tecnologías** para avanzar hacia un mundo más saludable, más pacífico, más solidario, más justo y más respetuoso con el medio ambiente, en el que se respeten los derechos de todos los niños y niñas.

6. **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 sólo podrán ser restringidos para garantizar la protección de los niños y niñas de informaciones y materiales 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.

7. **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, como restricciones de contenidos, lucha contra los abusos, limitaciones de acceso, etc.

8. **Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia** de todo tipo que se produzcan utilizando Internet. Los niños y niñas tendrán el derecho de utilizar Internet para protegerse de esos abusos, para dar a conocer y defender sus derechos.

9. **Los padres y madres tendrán el derecho y la responsabilidad de orientar, educar y acordar con sus hijos e hijas un uso responsable de Internet:** establecer tiempos de utilización, páginas que no se deben visitar o información que no deben proporcionar para protegerles de mensajes y situaciones peligrosas, etc. Para ello los padres y madres también deben poder formarse en el uso de Internet e informarse de sus contenidos.

10. **Los gobiernos de los países desarrollados deben comprometerse a cooperar** con otros países para facilitar el acceso de éstos y sus ciudadanos, y en especial de los niños y niñas, a Internet y otras tecnologías de la información para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los pobres.

unicef

ANEXO 3.

NETIQUETA

netiquétate

¡¡Apúntate a la Netiqueta Joven para Redes Sociales!!

1. Pide permiso antes de etiquetar fotografías subidas por otras personas

2. Utiliza las etiquetas de manera positiva, nunca para insultar, humillar o dañar a otras personas

3. Mide bien las críticas que publicas. Expresar tu opinión o una burla sobre otras personas puede llegar a vulnerar sus derechos e ir contra la Ley

4. No hay problema en ignorar solicitudes de amistad, invitaciones a eventos, grupos, etc.

5. Evita la denuncia injusta de SPAM para no perjudicar a quienes hicieron comentarios correctos

6. Usa las opciones de denuncia cuando esté justificada la ocasión

7. Pregúntate qué información de otras personas expones y asegúrate de que no les importa

8. Para etiquetar a otras personas debes hacerlo sin engaño y asegurarte de que no les molesta que lo hagas

9. No puedes publicar fotos o vídeos en las que salgan otras personas sin tener su permiso, como regla general

10. Antes de publicar una información que te han remitido de manera privada, pregunta si la puedes hacer

11. Facilita a los demás el respeto de tu privacidad e intimidad. Comunica a tus contactos, en especial a los nuevos, cómo quieres manejarlos

12. Recuerda que escribir todo en mayúsculas puede interpretarse como un grito

13. Usa los recursos a tu alcance (dibujos, símbolos, emoticonos..) para expresarte mejor y evitar malentendidos

14. Ante algo que te molesta, trata de reaccionar de manera calmada y no violenta. Nunca actúes de manera inmediata ni agresiva

15. Dirígete a los demás con respeto, sobre todo a la vista de terceros

16. Lee y respeta las normas de uso de la Red Social

www.netiquetate.com

ANEXO 4.

DIMENSIONES Y COMPETENCIAS INTELIGENCIA DIGITAL

DQ Institute, 2019, p. 12.

ANEXO 5.

CIBERACOSO

Gráfico de palabras de participantes en entrevistas grupales para construcción Protocolo.

ANEXO 6.

MANIFESTACIONES DEL CIBERACOSO

Gráfico de palabras de participantes en entrevistas grupales para construcción Protocolo.

ANEXO 7.

PREVENCIÓN DEL CIBERACOSO

Gráfico de palabras de participantes en entrevistas grupales para construcción Protocolo.

La educación es de todos

Mineducación

CISP
COMITATO INTERNAZIONALE PER LO SVILUPPO DEI POPOLI