Área Gestión de la convivencia en los centros docentes

Grupo Ciberacoso escolar

Servicio de Inspección Educativa

EL CIBERACOSO ESCOLAR Y SU REPERCUSIÓN EN LOS CENTROS EDUCATIVOS

GOBIERNO DEL PRINCIPADO DE ASTURIAS

CONSEJERÍA DE EDUCACIÓN

Tabla de contenido

1 Introducción al ciberacoso escolar

Las Tecnologías de la Información y de la Comunicación (TIC) y el uso cotidiano de internet tanto a nivel familiar como educativo, han supuesto un punto de inflexión en nuestra sociedad actual y también en el entorno escolar y educativo, afectando a múltiples aspectos de la convivencia y poniendo a nuestra disposición nuevas herramientas, cuya utilización, aunque generalmente satisfactoria, no está exenta de determinados riesgos que debemos conocer y por tanto prevenir.

Nuestros niños y adolescentes han nacido y viven en un mundo en el que lo virtual y lo analógico se confunden, pierden sus límites y contornos, y en el que no siempre existen las garantías necesarias para su adecuado uso y utilización, tanto en el entorno escolar como familiar. Por ello, la educación y su función en nuestra sociedad deben prevalecer sobre cualquier otro planteamiento y contribuir de forma decisiva a establecer los escenarios adecuados para el mejor desarrollo y formación de nuestro alumnado.

Uno de los cambios más importantes que ha provocado la irrupción de las nuevas tecnologías de la información y la comunicación, es el que se refiere a la forma de relacionarse de los adolescentes con sus iguales. Los teléfonos inteligentes o smartphones, las redes sociales y las aplicaciones de mensajería instantánea han transformado en poco tiempo la intensidad y el modo en que se interrelacionan los adolescentes y jóvenes, favoreciendo una conexión inmediata y permanente, sin necesidad de que medie el contacto directo o físico con las otras personas. Internet se ha convertido para nuestro alumnado, en un espacio clave para su socialización e interacción social, mediante el cual canalizan su comunicación y relaciones con sus iguales. A través de las redes sociales (Facebook, Twitter, Instagram) o mediante aplicaciones para teléfonos móviles como WhatsApp, los alumnos/as están continuamente conectados con sus compañeros/as, comentan sus vivencias diarias, comparten fotos o videos, expresan sus sentimientos y realizan comentarios de otras personas.

Como contrapartida de las enormes oportunidades de comunicación y aprendizaje que ofrecen las tecnologías de la información y la comunicación a nuestro alumnado, las mismas están ocasionando la aparición de "*nuevas formas de acoso"* en el entorno escolar, y concretamente una nueva forma de violencia entre iguales, denominada ciberacoso o *"cyberbullying",* con el agravante de que este nuevo comportamiento está siendo muy difícil de detectar y prevenir, por parte de familias y centros educativos.

Debido al impacto negativo que este nuevo fenómeno puede causar a la convivencia en los centros y a la creciente sensibilización de la sociedad, es necesaria una búsqueda activa de nuevas soluciones. Para ello, un primer paso es definir la realidad y caracterización de este nuevo concepto, así como las características del alumnado implicado, las causas y consecuencias del ciberacoso en sus diferentes manifestaciones y cómo corregirlas. También será objeto de este estudio, proporcionar a los centros educativos herramientas operativas y sencillas para la prevención positiva y detección temprana del ciberacoso escolar, así como a

creación de entornos seguros para el alumnado en plataformas de uso diario, como Microsoft Teams.

El objetivo final de este trabajo es sin duda alguna, contribuir a mejorar el contexto educativo, mediante una convivencia positiva que tenga como base el diálogo y la mediación como base para la resolución de conflictos.

2 Objetivos del trabajo

La definición de los objetivos propuestos, están formulados de forma amplia, al objeto de poder englobar el mayor número de apartados posibles, sin entrar en la concreción de objetivos operativos.

1. Comprender el fenómeno del ciberacoso escolar dentro de la sociedad actual, estableciendo prioridades básicas al objeto de atajar y prevenir esta situación, tanto en el marco educativo como familiar.
2. Establecer el marco legislativo general y autonómico en el que se contempla el fenómeno de ciberacoso escolar y su relación con el tratamiento de la convivencia en la Ley Orgánica 3/2020 de 29 de diciembre de 2020 (LOMLOE).
3. Efectuar un breve estudio comparativo en relación con el tratamiento del ciberacoso escolar a nivel de otras entidades educativas autonómicas.
4. Definir el concepto de ciberacoso escolar estableciendo con claridad las características y repercusiones que este nuevo fenómeno está originando tanto en el entorno familiar como a nivel educativo.
5. Proporcionar pautas necesarias para la adecuada actualización de los documentos institucionales de los centros educativos en relación con la prevención y tratamiento del ciberacoso escolar.
6. Establecer cauces efectivos destinados a la prevención positiva y detección temprana del ciberacoso escolar, acercando a los centros educativos conceptos como ciudadanía e identidad digital y su relación con el plan digital de centro, así como otras tecnologías destinadas a la comunicación y el aprendizaje del alumnado.
7. Promover el uso responsable de las TIC en los centros educativos creando un entorno seguro para el alumnado en el uso y manejo de *Microsoft Teams* y otros servicios digitales no institucionales.
8. Elaborar un protocolo de actuación sencillo y operativo destinado a la prevención y tratamiento del ciberacoso escolar, concretando modelos de actuación y distribución de responsabilidades entre familia, escuela y otros organismos públicos.
9. Poner a disposición del Servicio de Inspección Educativa las conclusiones de este estudio, con la posibilidad de incorporar los materiales elaborados, en futuras actuaciones, con el fin de mejorar la convivencia en los centros educativos

3 Definición y caracterización del ciberacoso escolar

El ciberacoso es un problema actual y emergente en nuestros colegios e institutos, crecientemente reconocido por la gran mayoría de los profesores y por la mayoría de los padres y madres que detectan y temen estos "*nuevos*" peligros.

Una de las primeras definiciones de ciberacoso ha sido presentada por Willard (2007) que dice que el acoso cibernético es enviar o disponer de material online con intención de perjudicar a los demás, o cuando hay intervención y participación en alguna forma de crueldad social a través de Internet o cualquier otra tecnología digital.

Li (2010), retomando la definición de Willard, enfatiza el uso de las TIC y se refiere al ciberacoso como un comportamiento que va más allá del envío o publicación de texto, donde se recurre también a imágenes perjudiciales y crueles a través de Internet y otros *"digital communication devices"* (medios de comunicación digital).

Por otro lado, Ortega et altri (2012) caracterizan el ciberacoso como una forma de acoso que usa tecnologías como el email, el móvil, los mensajes escritos, fotos, mensajes instantáneos, redes sociales y *"páginas web personales, con el propósito de hacer daño a otra persona a través de una actitud constante de hostilidad"*.

La comprensión del ciberacoso está directamente conectada a la tecnología de comunicación utilizada (email, sms, mms, chats, fotos, redes sociales como Hi5 o Facebook, Twitter) (Zych et altri, 2016).

El ciberacoso no tiene unas características estables. La literatura previa (Calmaestra et altri, 2010; Willard, 2007) establece los siguientes comportamientos:

- Manifestación de odio, amenazas, intimidación (*Flaming/Threats/Intimidation*);
- Insultos (*Bashing*);
- Asedio (*Online harassment*);
- Difamación/denigrar (*Denigration/Put Down/Misinformation*);
- Ciberpersecución (*Cyberstalking*);
- Bofetón alegre (*Happy slapping*): provoca deliberadamente situaciones de violencia con el fin de grabar en vídeo y divulgar las imágenes por Internet, teléfono móvil, etc.;
- Revelar secretos/chantajear (*Outing/Blackmail*);
- Exclusión (*Exclusion*);
- Disimulación/usurpación de identidad (*Posing/Masquerable/Identity Theft*);
- Insinuarse o hacerse amigo (*Trickery/Posing as a friend*);
- *Sexting*: enviar mensajes de carácter sexual

Ante la proliferación de casos detectados en los centros educativos, surge la necesidad de buscar medios formativos que nos ayuden a prevenir este tipo de situaciones problemáticas y de riesgo. Mediante una metodología inclusiva, donde se promueve el aprendizaje basado en la participación e inclusión del alumnado, cada vez son más los centros que optan por aplicar iniciativas o programas para luchar contra la vulnerabilidad de nuestros estudiantes a través del uso de los dispositivos móviles. No obstante, si bien nuestro propósito es erradicar el ciberacoso, antes debemos estudiar y conocer qué perfiles podemos encontrar en cuanto a víctimas y agresores para posteriormente diseñar nuestros programas formativos.

Asociado a la comprensión del concepto de ciberacoso y de los comportamientos o formas específicas en que el mismo se realiza, ha surgido la preocupación de caracterizar

comportamental y psicológicamente a las víctimas, los agresores y los que son simultáneamente una cosa y otra (Hinduja y Patchin, 2009; Olweus, 2000; Willard, 2007).

3.1 Caracterización de las víctimas

Los factores de vulnerabilidad con mayor incidencia son: la edad y año de escolaridad, el sexo, la orientación sexual, el ambiente familiar y etnia, algunos rasgos psicológicos y psicosociales – como la falta de amigos.

En cuanto a la edad de los practicantes del ciberacoso, se verifican disparidades relevantes en las investigaciones. Smith et altri (2008) no han encontrado relación. Algunos estudios señalan que la víctima está más expuesta a ciberacoso durante la adolescencia (Hinduja y Patchin, 2009; Patchin e Hinduja, 2010) y que después de este periodo la exposición disminuye (Bauman, 2010). Contrariamente, Slonje y Smith (2008) concluyen que el porcentaje de víctimas es menor entre estudiantes de los 15 a los 18 años, mientras es mayor entre los más jóvenes (12 a 15 años).

Sobre el sexo, la investigación previa no ha encontrado conclusiones consensuadas en los distintos estudios. Por ejemplo, según Smith et altri (2008) e Hinduja y Patchin (2009), las chicas tienen mayor tendencia a estar involucradas en situaciones de ciberacoso (más que en acoso directo) sea como víctimas, sea como agresoras; esto puede encontrar justificación a través de la tendencia de las chicas a implicarse en agresiones de carácter emocional más que físico. Sin embargo, para Wang (2013) esta inclinación se verifica en edades menores; aun así, según el mismo autor, al crecer los chicos pasan a ser más agredidos que las chicas. El estudio de Bauman (2010) indica que las chicas prefieren chats y mensajes instantáneos, mientras los chicos prefieren amenazar online y crear sitios web de odio. De acuerdo con Kowalsky et altri (2008), las chicas se implican más antes de la enseñanza media; después de este periodo se involucran al mismo nivel que los chicos. La orientación sexual de los jóvenes, cuando es diferente de la mayoría, parece ser también un gran factor en la vulnerabilidad, tal como ocurre en el acoso presencial.

En cuanto al ambiente familiar, la investigación es aún poco clarificadora, pero es muy probable que este sea también un factor importante, en la medida en que se revela una relación inversa entre el clima familiar y la supervisión parental y las prácticas de acoso (Bauman, 2010). Los niños de familias monoparentales parecen más expuestos a la victimización (Sourander et altri, 2010).

Finalmente, son variados los factores de orden psíquico y psicosocial que pueden considerarse predictores fundamentales de victimización. En general, en las víctimas se verifica un elevado nivel de ansiedad social y baja autoestima (Kowalski et altri, 2008; Patchin y Hinduja, 2010). Del Barrio (2013) confirma que los jóvenes con problemas de naturaleza afectiva están frecuentemente expuestos a la victimización. Según Vandebosch y Cleemput (2009), Sourander et altri (2010) y Sahin et altri (2012), las víctimas de ciberacoso crean más comportamientos depresivos hostiles, son más dependientes de Internet, se sienten menos populares y se arriesgan más con el uso de Internet. Este último aspecto es también relevante

para la relación entre victimización y el tipo de tecnología usada. Ybarra y Mitchel (2004) han concluido que las víctimas tienden a usar más que los jóvenes no-víctimas, los mensajes instantáneos, blogs y chats. *El estudio de Willard* (2007), a su vez, revela que los que están conectados a redes sociales (*Social Network Sites*, SNS) son más vulnerables a la victimización. Bauman (2010) considera que, debido a su dependencia de Internet, las víctimas soportan mejor las agresiones a las que están expuestas que la posibilidad de estar desconectado de las tecnologías. Esto tal vez sea un factor explicativo de su silencio, ya que tienen miedo de que les sean retirados los medios de acceso. También las víctimas de acoso tienen mayor tendencia a ser víctimas de ciberacoso (Sourander et altri 2010). Sin embargo, el sentimiento de inseguridad de las víctimas es más intenso en ocasiones de ciberacoso *"también porque el entorno del ciberacoso, siendo muy reciente, muchas personas no saben cómo poner término a la victimización"* (Sourander et altri, 2010).

3.2 Caracterización de los agresores o *bullies*

Li y Beran (2005) han verificado que los agresores de acoso tienden a ser también *cyber-agresores* y *cyber-víctimas*. Los agresores son caracterizados como niños y jóvenes mal adaptados desde un punto de vista psicosocial (bajo nivel de comportamientos pro-sociales), con baja autoestima e hiperactividad (Patchin y Handuja, 2010; Sourander et altri, 2010; Vandebosch y Cleemput, 2009). La disposición para el vandalismo, robo, consumo de tabaco y alcohol, escaparse del colegio y otras actuaciones de riesgo son también confirmadas (Pandori, 2013). Parece existir una fuerte asociación entre ser víctima (incluso en entorno presencial) y ser, posteriormente, agresor vía Internet o móvil (Vandebosch y Cleemput, 2009; Sourander et altri, 2010). Bauman (2010) verificó que la mayoría de los implicados en ciberacoso han sido también víctimas de acoso o agresores en el acoso presencial. Parece que las víctimas de acoso presencial ven en el anonimato, facilitado por las tecnologías, una forma de venganza de sus agresores (Ybarra y Michel, 2004); Sourander et altri (2010) confirman esta hipótesis sobre todo en las chicas. Es el grupo con más problemas psiquiátricos y psicosomáticos, con fuerte inclinación para la depresión, ansiedad y estrés (Sourander et altri, 2010). De acuerdo con el estudio de Vandebosch y Cleemput (2009) las víctimas-bullies se caracterizan por su falta de interés escolar, baja autoestima, y comportamientos problemáticos tales como vandalismo, choques con la policía, asaltos, robos, consumo de alcohol y tabaco.

4 Marco normativo de aplicación

4.1 Normativa básica

4.2 Normativa autonómica

5 Actualización de los documentos institucionales del centro

6 La prevención del ciberacoso escolar

6.1 Prevención positiva y detección temprana

La prevención del ciberacoso debe estar integrada como una actuación más en el Plan Integral de Convivencia, tal como se menciona en el Decreto 249/2007, de 26 de septiembre, por el que se regulan los derechos y deberes del alumnado y normas de convivencia en los centros docentes no universitarios sostenidos con fondos públicos del Principado de Asturias. A su vez, debe reforzarse de forma transversal desde el currículo y otras actuaciones que puedan desarrollarse en los centros educativos que contribuyan a mejorar la convivencia positiva y la participación de todos los miembros de la comunidad educativa en los centros.

Nuestro alumnado utiliza las tecnologías digitales con facilidad y agilidad sorprendentes, con asiduidad y de forma natural. Los adultos, sin embargo, nos acercamos a ellas con cierto recelo, temiendo ser superados por aquellos que pueden sorprendernos y dejar en evidencia nuestras inseguridades y desconocimiento del medio. Y, sin embargo, debemos acompañarlos y guiarles para que ese profuso uso se desarrolle en márgenes de responsabilidad, pensamiento crítico, ética y valores, seguridad, eficacia y eficiencia. Y este acompañamiento debe iniciarse desde la Educación Primaria y debe desarrollarse en un contexto de motivación y comunicación entre las partes (alumnado, familia y centro educativo) que permita tratar el tema con confianza y actuar de forma proactiva ante posibles casos de ciberacoso.

6.2 La educación digital

En este apartado se destaca la importancia de una correcta educación digital, a la que nuestro alumnado tiene derecho, guiándoles en la construcción de su identidad digital e integrando ésta en comunidad, entre iguales y con terceros, en lo que denominaremos incorporación a la ciudadanía digital.

El apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en su letra L, recoge como uno de los fines del sistema educativo español:

*"La capacitación para garantizar la plena **inserción del alumnado en la sociedad digital** y el **aprendizaje de un uso seguro de los medios digitales** y **respetuoso** con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva."*

A su vez la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de 6 de diciembre de 2018, en su artículo 83, establece el **derecho a la educación digital.** En este sentido determina que el sistema educativo debe garantizar *"la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales".*

Esta última ley recoge en su disposición adicional decimonovena sobre los derechos de los menores ante Internet que la administración deberá promulgar una ley dirigida específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

6.2.1 Agentes de la educación digital

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de 6 de diciembre de 2018, establece:

- En su artículo 84, sobre protección de los menores en Internet, que los **padres, madres, tutores, curadores o representantes legales** procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.
- En su artículo 92, sobre protección de datos de los menores en Internet, que los **centros educativos y cualesquiera personas física o jurídicas que desarrollen actividades en las que participen menores de edad** garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
- En su artículo 83, sobre el derecho a la educación digital, que las **Administraciones educativas** deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.
- En su artículo 83, sobre el derecho a la educación digital, que el **profesorado** recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

6.2.2 Funciones de los agentes de la educación digital

6.2.2.1 Familia

Como se ha señalado al mencionar los agentes que debe intervenir en la educación digital, los **padres, madres, tutores, curadores o representantes legales** procurarán que los menores de edad hagan un uso equilibrado y responsable de la tecnología y de los servicios que utilizan esta.

Función de tutelaje y supervisión. Debe ejercer un control del uso que sus hijos e hijas hagan de los medios, especialmente en las etapas inferiores del sistema educativo, en la que se sientan las bases para su correcto uso y se crean hábitos saludables.

Función de formación. El correcto uso de la identidad digital del alumnado y de las herramientas tecnológicas es básico. Hay que tener en cuenta que las propias familias pueden no estar preparadas para desarrollar con eficacia esta función.

6.2.2.2 Centro educativo

Función de supervisión. Las conversaciones dentro de los canales de los equipos de clase deben someterse a auditoría periódica para detectar conductas inapropiadas. Por definición los chats y conversaciones en canales son permanentes, de forma que el intercambio de mensajes se va acumulando con el tiempo. Los canales, además, permiten cierta configuración desde su correspondiente administración dentro de cada equipo. Estudiar las mejores opciones para evitar conductas inapropiadas. Hay que buscar las evidencias.

Función de formación y sensibilización. Uso responsable de la identidad digital y de los servicios asociados a ella. Complementaria a la que se pueda realizar desde la familia. Incluida en el plan de digitalización para todos los sectores de la comunidad educativa. Más que evitar, es hacer un uso responsable e indicar que nuestra actividad en Internet deja un rastro que se puede seguir.

6.2.2.3 Administración

Función de formación y sensibilización. La administración educativa debe definir en el currículo los contenidos, valores y competencias transversales necesarias para el uso adecuado, responsable y respetuoso de los medios tecnológicos. Asimismo, deben garantizar la formación del profesorado necesaria para la correcta transmisión de esos valores y la propia competencia digital docente.

Función de administración. La Consejería de Educación, a través de Educastur como área responsable de los servicios educativos en línea, y en colaboración con la Dirección General de Seguridad y Estrategia Digital, está tomando medidas para atajar, minorar y anticiparse a conductas inapropiadas, acotando el uso que el alumnado pueda hacer de los medios tecnológicos institucionales.

El contacto frecuente con los centros educativos permite a la Consejería conocer posibles actuaciones no deseadas y buscar la mejor respuesta a estas, por lo que es necesaria la coordinación permanente entre ambos agentes.

6.3 Ciudadanía e identidad digital

El uso de Internet en nuestros centros educativos es una realidad. No es un proceso opcional o complementario, es necesario y está imbricado en la acción educativa. También en el contexto familiar. En ambos ámbitos es necesario definir y modelar el uso responsable y la gestión de la identidad digital, como elementos imprescindibles de la ciudadanía digital y la formación de la personalidad en la red de los alumnos.

Esta realidad precisa de “un desarrollo competencial, digital, en todos los agentes implicados: las direcciones de los centros educativos, sus profesores, alumnos y familias” (Tourón, 2021).

Se trata, por tanto, de adquirir los conocimientos y herramientas necesarias para el fomento de la convivencia digital responsable y la protección de los menores en Internet. El ciberacoso y la violencia digital temprana deben combatirse desde la prevención y la educación, dando voz y protagonismo a todos los integrantes de la comunidad escolar. El ciberacoso escolar es, probablemente, uno de los problemas a los que se enfrenta un mayor número de menores. (Haro Ollé, 2020)

6.3.1 Identidad digital

La identidad digital es todo aquello que nos identifica en Internet y, por tanto, nos define. A medida que utilizamos diferentes herramientas, redes sociales o sistemas de mensajería, cada uno de nosotros va dejando una huella que es visible por cualquiera con acceso a un buscador o a nuestros perfiles en redes (Haro Ollé, 2020).

Se refiere a los aspectos de la tecnología digital como mediadora en la experiencia de la identidad construida por las personas y también condicionada por factores sociales (Castañeda; Camacho, 2012). Estas mismas autoras definen dos partes bien diferenciadas de esta identidad digital. Una primera parte es la personal que respondería a la pregunta ¿Qué enseño sobre mí mismo en Internet? La segunda parte es la social, que respondería a las preguntas ¿Quién me influencia? y ¿Quién se ve influenciado por mí?

Como se puede apreciar, tan importante es conformar una sólida identidad digital como establecerla en un contexto sano, seguro y respetuoso de interrelación con terceros. El uso responsable de Internet no es un acto individual y aislado, sino que tiene repercusiones en muchas otras personas y, a diferencia del mundo analógico, estas repercusiones tienen un alcance mucho mayor, más rápido y en personas que pueden estar muy alejadas físicamente de nosotros. Se trata, por lo tanto, de un nuevo ecosistema social que es necesario aprender a manejar y gestionar (Haro Ollé, 2020).

6.3.2 Ciudadanía digital

Existe una nueva responsabilidad que ha aparecido en siglo XXI: la de saber ser ciudadano digital. Los niños tienen acceso a Internet desde muy pequeños y deben saber desenvolverse en este ámbito. Igual que se enseña cuándo se debe cruzar la calle y cuándo no, también tienen que saber qué se puede hacer y qué no en Internet (Haro Ollé, 2020).

Se reconocen como habilidades propias de un buen ciudadano digital aquellas que definen un usuario activo en la red, que usa intensivamente las tecnologías de la información, que es creador de contenido más allá que puro consumidor, que interactúa con usuarios y organizaciones y que utiliza servicios de comercio electrónico, de banca online, de información, etc. Nuestro alumnado debe ir preparándose para una incorporación progresiva a la ciudadanía digital. Al resto de agentes nos corresponde definir claramente las habilidades que debe adquirir el alumnado en esa incorporación. «Un ciudadano digital es aquella persona que utiliza tecnología de la información para mejorar su participación en la sociedad, la política y el gobierno, o sea, los que utilizan Internet regularmente y con efectividad». (González, 2019)

Como se ha venido demostrando, la escuela tiene un efecto compensador en busca de la necesaria equidad que minimice la brecha digital. Debe identificar a aquel alumnado con dificultades en el acceso a Internet y facilitarles el uso de la tecnología en el aula. A la vez, debe darles las competencias necesarias para su manejo pues, aunque se les reconoce como nativos digitales (Prensky, 2001), esa temprana iniciación al medio no va acompañada de la necesaria habilidad para su uso de forma eficiente y responsable.

Mejorar los procesos de orientación como método de mejora de la identidad digital bajo un escenario de responsabilidad puede convertirse en el mejor aliado tanto para la prevención como para la mejora en los usos de internet. Ante todo, es necesario potenciar el uso ético de los entornos virtuales, y no sólo a edades tempranas (Bermejo, 2017).

6.3.3 Relación con el Plan Digital de Centro

El Plan Digital de Centro se entiende como un instrumento que debe favorecer e impulsar el uso de los medios digitales tanto en los procesos de enseñanza-aprendizaje como en el resto de los procesos de gestión del centro, siempre con el objetivo último de colaborar en el desarrollo integral del alumnado (INTEF, 2020).

Las instituciones educativas tienen que revisar sus estrategias organizativas para mejorar su capacidad de innovación y para explotar todo el potencial de las tecnologías y contenidos digitales (Kampylis; Punie; Devine, 2015). La digitalización de los centros educativos toma como referencia el Marco Europeo para Organizaciones Educativas Digitalmente Competentes (DigCompOrg). Según los elementos de este marco, se proporcionan algunas orientaciones de carácter general para identificar actuaciones necesarias en relación con los siguientes ámbitos o ejes temáticos: las infraestructuras, el liderazgo y la gobernanza, el proceso de aprendizaje y enseñanza, el desarrollo profesional; los contenidos, la evaluación y las redes de apoyo y colaboración.

Como se ha venido describiendo en este apartado, los centros educativos deben ayudar a su alumnado a conformar su identidad digital y a incorporarse progresivamente a la ciudadanía digital. El Plan Digital de Centro ayuda en la consecución de estos fines. Tanto las habilidades y contenidos necesarios como la participación de los agentes en su desarrollo aparecen de forma transversal en muchos de los ámbitos del plan:

- El personal y el alumnado son digitalmente competentes (Proceso de aprendizaje y enseñanza).
- Se ponen en primer plano la seguridad, los riesgos y un comportamiento responsable en entornos en línea (Proceso de aprendizaje y enseñanza).
- Se espera la colaboración entre los diversos agentes y el trabajo en grupo (Redes de apoyo y colaboración).
- Se desarrollan destrezas sociales y emocionales: las destrezas necesarias para entender y gestionar emociones, establecer y alcanzar objetivos positivos, sentir y mostrar empatía por otras personas, establecer y mantener relaciones positivas y tomar decisiones responsables y guiadas por un pensamiento crítico (Proceso de aprendizaje y enseñanza).

- Se respetan los derechos de propiedad intelectual y de copyright (Contenido y currículos)
- Hay establecida una Política de Uso Aceptable, protección de datos y cumplimiento legal (Infraestructura)
- Están claras las medidas para proteger la privacidad, la confidencialidad y la seguridad (Infraestructura)

6.4 Tecnologías para la comunicación y el aprendizaje

La transformación digital de la educación es un proceso irreversible que ha tenido una aceleración significativa en este último año. La tecnología puede y debe contribuir a introducir metodologías activas en el aula que permitan construir un aprendizaje eficaz, natural y fluido, equitativo, atractivo y motivador, ubicuo y permanente. En este sentido, el profesorado tiene acceso a un elevado número de servicios y aplicaciones que las facilitan. Las dos principales plataformas institucionales lo consiguen con sus propios medios y características.

Pero el aprendizaje en línea puede presentar desafíos de seguridad únicos para el alumnado. Es una gran oportunidad para que el alumnado pueda crear y practicar la ciudadanía digital junto con su aprendizaje académico.

6.4.1 Servicios digitales no institucionales

La Dirección del Centro docente es la responsable de las aplicaciones informáticas, apps de móvil y servicios en línea que utilice el profesorado y alumnado en el entorno escolar y que recaben datos personales.

A este respecto, y por la responsabilidad que implica para los prestadores y usuarios de los servicios educativos, se recomienda la atenta lectura de la documentación disponible en https://www.educastur.es/en/proteccion-datos:

- Normativa europea: Reglamento General de Protección de Datos (RGPD) (DOUE 04/05/2016, en vigor desde el 25 de mayo de 2018.
- Normativa española sobre protección de datos de carácter personal.
- Recomendaciones publicadas por la Agencia Española de Protección de Datos para los centros docentes.
- Informe sobre uso de aplicaciones de dispositivos móviles y aplicaciones en la nube desarrollado por el Servicio de Inspección educativa.

El número de aplicaciones y servicios web a disposición del profesorado fuera del entorno institucional es muy importante. Se aleja del alcance de este documento la posibilidad de estudiar cada uno con detalle para ver en qué medida se pueden arbitrar configuraciones de seguridad adecuadas para limitar el uso no deseado. En todo caso, se ha de dedicar tiempo a su conocimiento y configuración, velando porque la incorporación de las tecnologías en las aulas se realice respetando el derecho a la protección de datos de aquellos cuya información personal se trata.

Las aplicaciones utilizadas deberían permitir el control por parte de los tutores y las tutoras o profesorado de los contenidos subidos por los y las menores. Además, deberían establecerse programas informativos de concienciación para profesorado y alumnado sobre protección de datos y la importancia del uso correcto de esas aplicaciones, sobre todo en lo concerniente a la publicación de contenido y configuración de las opciones de privacidad.

6.4.2 Servicios digitales institucionales

La Consejería de Educación pone a disposición de la comunidad educativa una serie de servicios en línea de uso profesional y educativo de carácter institucional, así como las identidades digitales de acceso a estos para centros, profesorado y alumnado. Por su carácter institucional, y para evitar conflictos o usos inadecuados de software y datos personales, se recomienda que todos los perfiles educativos (centros, profesorado y alumnado) utilicen prioritariamente estos servicios.

Los servicios en línea y plataformas en la nube para uso educativo con alumnado y la formación a distancia de carácter institucional disponibles en la fecha de publicación de este documento, son los siguientes:

- Campus Aulas Virtuales y FP distancia.
- Microsoft 365

Se debe formar al alumnado en, al menos, una de esas plataformas y se debería unificar el uso de una única plataforma para el mismo grupo de alumnos de forma que no tengan que usar distintas plataformas para cada asignatura.

A continuación, se describe *Microsoft Teams* y cómo crear un entorno seguro en este servicio por ser el de uso más extendido en nuestra comunidad autónoma.

6.4.3 Microsoft Teams

Microsoft Teams es una herramienta multifuncional que conforma un espacio de trabajo. Por un lado, es una herramienta de comunicación, por otro, es una plataforma al servicio de la colaboración y el trabajo en equipo. La idea que subyace en esta aplicación es unir personas en torno a tareas comunes por lo que la interacción se convierte en un factor clave. Crear, gestionar y trabajar en equipo es muy sencillo gracias a las herramientas que ofrece *Teams* y a la integración de estas herramientas entre sí que nos proporciona *Microsoft 365*.

Entre los diferentes contextos de comunicación que permite *Microsoft Teams* podemos encontrar momentos en los que el alumnado interacciona entre sí. *Teams* ofrece espacios para la comunicación en forma de mensajería (chat) y en conversaciones en canales de equipos y en reuniones. Esta comunicación puede ser solo textual o incluir audio y vídeo.

Es en esa interacción donde se puede dar la posibilidad de que se dé algún tipo de situación que atente contra la convivencia, especialmente en aquellas en las que el adulto, bien en la figura del profesional docente, bien en la de la familia, no está presente. Las funciones de formación, tutelaje, modelaje y supervisión comentadas anteriormente son básicas para que el

uso de la herramienta sea el correcto y la comunicación se produzca en un contexto de respeto mutuo y de observancia de las normas establecidas. Estas deben ser siempre líneas prioritarias de nuestra actuación. No obstante, se dispone de ciertas directivas de seguridad que ofrece de serie *Microsoft Teams* al alcance de los centros y personal docente y de otras que pueden disponerse de forma centralizada por la propia administración educativa.

En el anexo 1 de esta guía se desarrolla este tema, describiendo cómo crear un entorno seguro para el alumnado en *Teams*.

7 Protocolos de actuación y tratamiento del ciberacoso

7.1 Modelos de actuación

Independientemente de que se manifieste o no en el contexto escolar, la comunidad educativa debe conocer cuál es la mejor forma de detectarlo, afrontarlo y erradicarlo, para poder así contribuir al desarrollo óptimo del alumnado.

Ésta no es tarea fácil debido a las singulares características del ciberacoso con las nuevas tecnologías: anonimato, inmediatez, efecto en cadena, alta disponibilidad, diversidad de canales y procedimientos, entre otros.

7.1.1 ¿Cómo defenderse del ciberacoso?

Como se ha descrito en el apartado referido a la prevención, todo el profesorado debe asumir su responsabilidad para transmitir las pautas necesarias para el uso seguro y responsable de Internet. En concreto, el correcto tratamiento de la ciudadanía e identidad digital ya descrito. Y, de forma más concreta:

- Sesiones formativas en el centro sobre el respeto entre iguales
- Enfatizar en el hecho de que Internet no es anónimo.
- Ofrecer al menor una figura responsable, del centro escolar, para acudir ante cualquier problema de convivencia.
- Estar alerta ante situaciones conflictivas que puedan derivar en ciberacoso.
- Conocer el Protocolo de actuación por si algún alumno fuera víctima de ciberacoso, prestando especial atención a no significar más a la víctima con nuestras actuaciones.

7.1.2 Protocolo de actuación ante casos de ciberacoso en el centro

Cualquier miembro de la comunidad educativa que sospeche o tenga conocimiento de un caso de ciberacoso en el centro debe comunicarlo al equipo directivo. El cual debe establecer los procedimientos específicos para la detección e intervención de este tipo de casos:

a) Valoración: se debe establecer un proceso de recogida de información que sirva para valorar el caso de ciberacoso.
b) Comunicación: una vez detectado un caso de ciberacoso, se debe comunicar a las familias de los alumnos implicados. La colaboración entre familia-centro es primordial.
c) Acciones de protección: establecer las medidas para proteger a la víctima y las pautas para tratar al ciberacosador.

Resaltar que cualquier integrante del a comunidad educativa, debe entregar la información que tenga al respecto. Los progenitores que se enteren de que su hijo es víctima de ciberacoso deben ponerse en contacto con el centro en forma inmediata. Si es posible, la familia o el agredido deben copiar de inmediato la página o imprimirla, para tener antecedentes que respalden lo sucedido. Se debe resguardar la privacidad de los alumnos y confidencialidad de la situación denunciada.

Los centros educativos en los casos de ciberacoso en el Principado de Asturias deben seguir el Protocolo de actuación ante el acoso escolar, regulado por la Circular del Consejero de Educación y Cultura sobre las instrucciones que regulan la aplicación del protocolo de actuación ante situaciones de posible acoso escolar en los centros docentes no universitarios de Asturias de 16 de marzo de 2018.

7.1.3 Consecuencias del ciberacoso. Legalidad y sentencias

En España el acoso escolar y el ciberacoso cuentan con una regulación a nivel penal. En concreto, nuestras leyes lo contemplan cuando al acoso se produce a través de medios digitales, es perpetrado entre menores y dentro de un contexto educativo.

El ciberacoso es un delito penal que puede acarrear cárcel, con penas de prisión de tres meses a dos años, o multa de seis a 24 meses. Si se acosa a una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se puede llegar a imponer la pena de prisión de seis meses a dos años (sin multa).

Cuando se trata de un menor, es importante recordar que la responsabilidad civil recaerá sobre los padres, siendo habituales las sentencias que obligan a **indemnizar a la víctima con 3000 euros o más**.

En el supuesto de que víctima y agresor hayan tenido una relación sentimental, o cuando los mensajes van dirigidos a descendientes, ascendentes, o a familiares del excónyuge, se impondrá una pena de prisión de uno a dos años, o bien trabajos en beneficio de la comunidad de 60 a 120 días.

7.2 Distribución de responsabilidades

7.2.1 Familias

Desde el punto de vista legal, según resalta el juez de Menores, Ernesto Mallo, “los padres tienen las obligaciones derivadas de la patria potestad que indica el Código Civil, de manera que es evidente que los padres, tanto por deber legal, como por sentido común, en cuanto tienen bajo su guarda a menores, deben estar atentos a las actividades que sus hijos realizan en Internet, y deben poner los límites necesarios.”

En el caso de que sus hijos/as cometan hechos delictivos, la Ley Orgánica 5/2000, de 12 de enero, de Responsabilidad penal de los menores, establece, en su artículo 61.3: “Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y

guardadores legales o de hecho, por este orden. Cuando estos no hubieren favorecido la conducta del menor con dolo o negligencia grave, su responsabilidad podrá ser moderada por el juez según los casos.", por lo tanto, en la responsabilidad civil, en el pago de las responsabilidades que pudiesen corresponder, actuarán de forma solidaria los padres juntamente con sus hijos.

7.2.2 Centros educativos

Código Civil. Artículo 1902. "*El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.*"

Código Civil. Artículo 1903. "*La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder. Los padres son responsables de los daños causados por los hijos que se encuentren bajos u guarda.*

Los tutores lo son de los perjuicios causados por los menores o incapacitados que están bajo su autoridad y habitan en su compañía.

Lo son igualmente los dueños o directores de un establecimiento y empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.

Las personas o entidades que sean titulares de un centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del centro, desarrollando actividades escolares o extraescolares y complementarias.

La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño."

7.2.3 Fiscalía

La denuncia puede llevarse a cabo ante: la policía, el Juzgado de Guardia o la Fiscalía de Menores.

En la jurisdicción de menores es el fiscal el que tiene la competencia para incoar (iniciar) o no un expediente de reforma (el expediente penal), y si lo incoa, es también el fiscal el que tiene la labor de instruirlo, tomando declaraciones, reuniendo pruebas, etc.

La labor del juez de menores comenzaría una vez terminada la fase de instrucción, para dar audiencia a las partes, hacer el juicio, dictar sentencia y ejecutarla si es condenatoria.

7.3 Herramientas, protocolos y guías

Estamos convencidos de que la primera actuación ante el acoso y ciberacoso debe ser preventiva, es decir, debemos actuar educativamente para evitar que se den situaciones de acoso o de ciberacoso. En este sentido, proporcionar a los docentes instrumentos sencillos de aplicar y codificar (que no sea necesaria de manera obligada la intervención del orientador/a del centro), podría ser un primer peldaño en la identificación de conductas que por su propia naturaleza y medio no son fácilmente observables en el aula.

7.3.1 Instrumento para la detección temprana de posibles casos de ciberacoso

Como aludíamos en el punto referido a la introducción del presente estudio, el ciberacoso es un fenómeno relativamente reciente dentro del contexto escolar y por sus propias características, muy difícil de prevenir y detectar. El carácter privado de muchas agresiones dificulta su identificación, siendo característico que la víctima de un acoso escolar no comunique su situación a sus profesores, compañeros y menos aún, a su familia.

Es por ello, que la línea de trabajo que proponemos en este apartado, pasaría en primer lugar, por la elaboración de un instrumento sencillo y fácil de aplicar por parte del profesorado, al objeto de poder prevenir posibles comportamientos de ciberacoso que puedan estar produciéndose entre el alumnado (y que no se han detectado), al objeto de poder actuar educativamente ante este tipo de conductas contrarias a las normas de convivencia del centro y poder aplicar medidas para la mejora de la convivencia y la resolución de conflictos.

En este sentido, nos parece conveniente mencionar el estudio efectuado por Abel Baquero Correa y Bertha Lucía Avendaño Prieto, *"Diseño y análisis psicométrico de un instrumento para detectar presencia de cyberbullying en un contexto escolar",* fruto del cual se publicó un instrumento de medida al objeto de identificar cualquier tipo de maltrato psicológico, verbal o físico, producido entre el alumnado de forma reiterada y prevenir posibles situaciones de ciberacoso dentro del ámbito escolar.

Un aspecto novedoso y muy útil a lo hora de establecer medidas preventivas y educativas, es que esta guía permite evaluar e identificar conductas referidas a posibles ciber agresores, determinando la existencia de una o varias víctimas y finalmente la presencia o no, de posibles espectadores (alumnos/as activos o pasivos) que están involucrados en este tipo de conducta.

Los últimos estudios efectuados sobre el tema apuntan que en el ciberacoso escolar suelen participar diferentes alumnos y alumnas que adoptan roles diferenciados y, al mismo tiempo, variables en función del contexto y del momento en el que se produzca. Para diferenciar bien las figuras que se dan y los roles posibles en el denominado *"triángulo del ciberacoso"* (víctimas, acosadores y espectadores pasivos/activos), es necesario atender a sus perfiles diferenciadores, al objeto de poder aplicar medidas de carácter preventivo, con la mayor prontitud que sea posible.

La guía en cuestión se publicó con un total de 24 indicadores, que finalmente para su aplicación en el ámbito educativo, se redujeron a 18 y que deben de ser respondidos con una escala Likert con tres niveles de respuesta.

N.º	Indicador	Nunca	Algunas veces	Bastantes veces
1	Alguna vez he utilizado redes sociales (WhatsApp, Instagram, Facebook, otros …) para reírme, ridiculizar, criticar a un compañero/a de clase			
2	He publicado, alguna vez, en redes sociales, defectos de compañeros/as que me caen mal			
3	He subido, alguna vez, a redes sociales imágenes ridículas de otros compañeros/as			

4	Alguna vez he amenazado a otro compañero/a utilizando el correo electrónico, redes sociales etc.			
5	Me divierto (entretengo) utilizando las redes sociales/correo electrónico para molestar o ridiculizar a compañeros/as			
6	Animo a otros compañeros/as a utilizar las redes sociales para reírme, molestar, ridiculizar etc. a conocidos/as y/o amigos/as			
7	He sido perjudicado/a con algún tipo de información falsa publicada en redes sociales			
8	Alguna vez alguien se hizo pasar por mí en redes sociales, al objeto de burlarse o decir algo de otros compañeros/as			
9	Alguien ha publicado alguna vez en redes sociales algún tipo de información (imágenes) de mi vida privada			
10	He recibido mensajes de texto ofensivos o burlándose de mí, en el teléfono, redes sociales, etc.			
11	He sido amenazado/a en redes sociales, correo electrónico, etc.			
12	Me siento muy mal por cosas (mensajes, imágenes etc.) que he recibido en mi teléfono o redes sociales			
13	Mis compañeros/as de clase saben que en las redes sociales se han burlado de mí			
14	Tengo conocimiento que algunos compañeros/as de clase utilizan las redes sociales, correo electrónico, teléfono móvil etc. para burlarse o reírse de otros/as			
15	Apoyo a mis compañeros/as cuando sé que están siendo molestados en redes sociales			
16	Observo con interés (sigo) las peleas/conflictos etc. que ocurren en las redes sociales, entre mis compañeros/as de clase			
17	Hay compañeros/as que participan habitualmente en las peleas/conflictos que se producen en las redes sociales			
18	Existe indiferencia entre mis compañeros/as de clase cuando molestan a otros/as en las redes sociales			

7.3.1.1 Descripción de los ítems

Los primeros seis ítems se refieren a **conductas típicas de un agresor/a** respecto a la utilización de las redes sociales para molestar, intimidar, amenazar, ridiculizar e incomodar a sus compañeros/as mediante comunicaciones hostiles o la publicación de materiales ofensivos.

Los siguientes seis indicadores están relacionados con percepciones de quienes han sido agredidos a través de redes sociales, los cuales **permiten identificar a las posibles víctimas** en una situación de ciberacoso.

Finalmente, los seis ítems restantes corresponden a conductas típicas **de los espectadores** (alumnos/as que pueden estar involucrados), de forma activa y/o pasiva, en una presunta situación de ciberacoso escolar.

7.3.1.2 Codificación de los ítems

- Nunca: 0
- Algunas veces: 1
- Bastantes veces: 2

7.3.1.3 Cuantificación de las respuestas

La cuantificación de las respuestas nos permite analizar los resultados obtenidos para cada categoría o grupo de ítems.

Indicadores del 1 al 6

1. La obtención **de 0 a 2 puntos en los primeros seis indicadores (perfil ciber agresor)**, nos indicarían **la ausencia significativa** de presuntos alumnos/as que estuviesen empleando conductas de maltrato psicológico hacia sus compañeros/as.
2. El rango obtenido **de 3 a 6 puntos** nos permitiría identificar la existencia de alumnos/as que, en algún momento, ha empleado las redes sociales para ridiculizar y/o agredir virtualmente a otro/a compañero/a de su clase. Este dato sería suficiente para empezar a aplicar medidas preventivas en el grupo al objeto de erradicar un presunto caso de ciberacoso.
3. La obtención de **más de 6** puntos indicaría la existencia de alumnos/as que podrían estar actuando de forma reiterada, con conductas claramente dirigidas a maltratar mediante entornos virtuales, a otros/as compañeros/as de su clase.

Esta misma escala se reproduce en los siguientes dos grupos de indicadores de esta guía.

Indicadores del 7 al 12

1. Una puntuación **entre 0 y 2 puntos** obtenida en estos ítems no indicaría la existencia de alumnado que se haya considerado agredido de una forma significativa y/o reiterada.
2. El rango **entre 3 y 6** nos alertaría sobre la presencia de alumnos/as que, en algún momento, han sido agredidos de alguna forma en redes sociales, o al menos se han sentido maltratados por sus compañeros en alguna ocasión, lo cual debería ser el momento adecuado para iniciar medidas de carácter preventivo y atender emocionalmente a este alumnado.
3. La obtención de **más de 6** puntos en este grupo de indicadores permitiría identificar a algún alumno/a que percibe de forma clara, la situación de víctima en una presunta situación de ciberacoso escolar.

Indicadores del 13 al 18

Por último, y en relación con la existencia de posibles espectadores, es decir, alumnos/as que son conocedores de posibles conductas constitutivas de ciberacoso y que puedan estar

involucrados de forma activa y/o pasiva en las mismas, se valoraría de manera análoga, a las categorías anteriores.

1. La obtención **de 0 a 2 puntos** en estos ítems no permitiría establecer la existencia de alumnado partícipe en una presunta situación de ciberacoso.
2. La cuantificación **de 3 a 6 puntos** nos alertaría sobre la presencia de alumnos/as que son conocedores/as y/o espectadores, de posibles comportamientos negativos en redes sociales o entornos virtuales, hacia sus iguales.
3. Una puntuación **superior a 6 puntos** en esta categoría nos indicaría la influencia que los presuntos agresores/as están ejerciendo sobre el grupo, y la existencia de alumnos/as que, inducidos por el contagio social, bien no hacen nada (se inhiben) o bien participan activamente en un posible caso de ciberacoso escolar.

7.3.2 Guía para la autovaloración del alumno

Guía para la autovaloración del alumno ¿Soy víctima de ciberacoso? ¿Qué puedo hacer? Guía para el análisis y la reflexión de los alumnos. (Material para uso didáctico del tutor) Propuesta para la reflexión de los alumnos en situaciones de conflicto por posible ciberacoso.

La presente guía de autorreflexión se propone como un documento de base que permitiría al profesorado testar con sus alumnos las dudas que ellos mismos pudieran tener sobre si determinadas situaciones deben o no ser consideradas como ciberacoso, así como las hipotéticas acciones a desarrollar. Se introduce también, como instrumento didáctico a desarrollar y personalizar en cada centro con las aportaciones que los propios alumnos (en actividades didácticas de prevención y sensibilización) puedan plantear en la secuencia de autoanálisis sugerida. Se entiende como un material a trabajar siempre con la supervisión de un adulto.

La edad de los alumnos, así como su madurez, son consideradas un factor básico para determinar los pasos a dar por una posible víctima de ciberacoso cuando tiene conocimiento por primera vez de una situación que encaja en el fenómeno de referencia.

Sin embargo, es indispensable establecer ciertos criterios para determinar si es necesario informar a los adultos a la primera señal de una agresión y si existe la posibilidad de actuar personalmente o con la ayuda de algún compañero para intentar detener lo que le afecta.

La normativa sobre consentimiento para el tratamiento de datos de carácter personal de menores de edad establece que a partir de los 14 años estos están habilitados a crear un perfil en una red social (y las acciones que de ello se derivan) sin el consentimiento expreso de los padres.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales aborda en su artículo 7 el consentimiento para el tratamiento de datos de los menores de edad:

> *1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los*

supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Podría utilizarse este parámetro citado como referencia para definir diferentes modos de actuar, en función de la edad, ante una supuesta situación de ciberacoso.

7.3.2.1 Secuencia de revisión de situaciones y toma de decisiones

Como propuesta a trabajar con los alumnos (extremando la prudencia), podría plantearse la siguiente secuencia de revisión de situaciones hipotéticas y toma de decisiones para adolescentes con edad superior a 14 años:

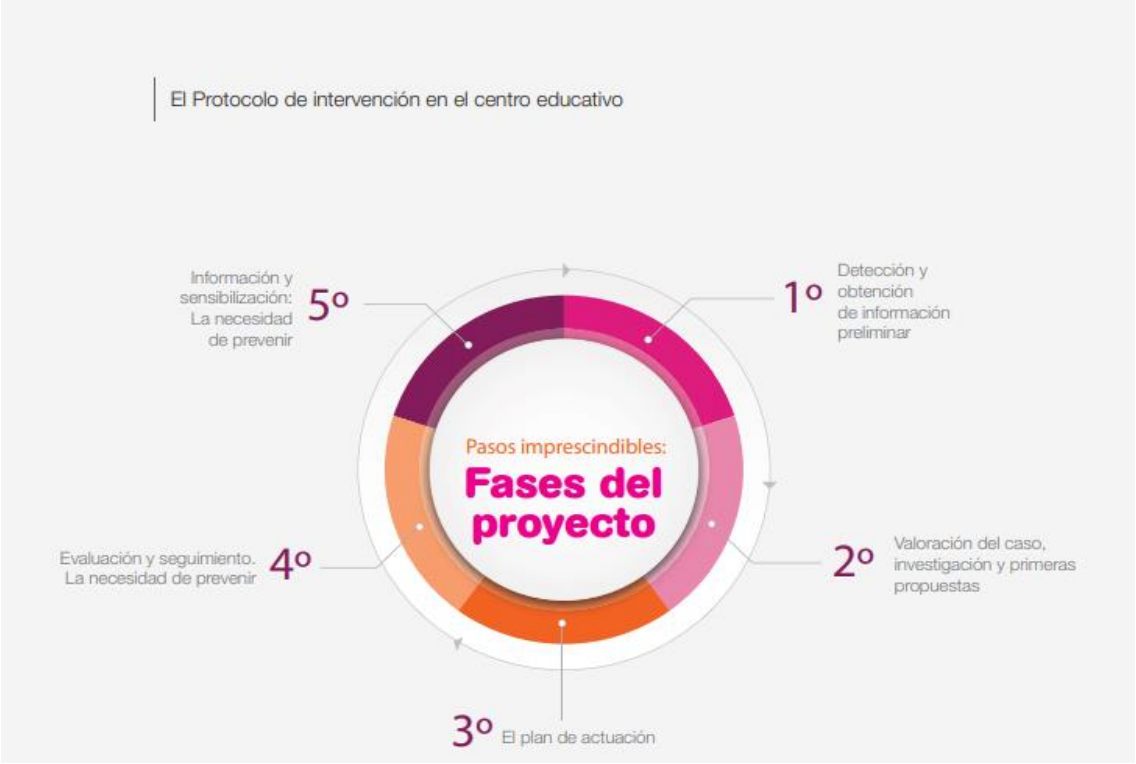
1. **Piensa y reflexiona.** Te enteras de que algún compañero puede estar haciendo cosas que te resultan ofensivas o desagradables utilizando para ello algún dispositivo tecnológico. Por ejemplo, alguien ha grabado y colgado imágenes tuyas sin tu consentimiento en una red social o en una página web de vídeos; observas que han retocado ofensivamente una foto tuya o que está etiquetada de manera insultante; se te insulta o veja a través del WhatsApp o en algún blog, foro o chat; han suplantado tu identidad en la red social o mensajería instantánea y te utilizan para mandar mensajes a otras personas.
2. **Analiza y valora lo sucedido**, y piensa cómo te afecta en lo personal y social. A veces, se trata de bromas que no siguen en el tiempo o que consideras, incluso, que no son importantes. Si consideras que, por el momento, no sabes muy bien qué pasa y quieres enterarte bien antes de decidir qué hacer, reúne información (paso 4).
3. Aunque no dispongas de muchos datos, si lo que vives te sorprende y te sientes ofendido y sin posibilidad de respuesta, **cuéntalo inmediatamente a tus padres y/o profesores**. Puede ocurrir que algún compañero te cuente lo que está pasando o que tú mismo lo hayas detectado pero que no dispongas de posibilidades de saber quién ha provocado la situación; puede que sepas quién te ha ofendido, pero no te atreves a decirle nada. En otras ocasiones te enteras tarde, cuando ya lleva tiempo diciéndose algo insultante de ti o utilizándose alguna imagen tuya sin consentimiento y de modo inadecuado, y no sabes cómo proceder… Si te sientes inseguro y dolido, informa de lo que conoces, aunque no tengas demasiada información.
4. **Reúne información** (no te deshagas de ella) sobre lo que consideras que, en principio, puede ser algo ofensivo hacia ti y cómo, y mediante el uso de qué medios tecnológicos ha sido. Reflexiona sobre cómo te sientes. Puedes hablar con algún compañero con el que tengas confianza. Pregúntate: a. ¿Qué ha pasado? b. ¿Cómo ha ocurrido?: procedimiento utilizado y difusión. ¿Cuándo ha ocurrido?: el comienzo. c. ¿Durante cuánto tiempo lleva produciéndose la situación? d. ¿Quién o quiénes han desarrollado la acción y quiénes la conocen? ¿Es o son conocidos los autores? e. ¿Existe alguna situación previa que creas ha podido originar la situación? f. ¿Qué crees que pretenden los autores con sus acciones?
5. **Escribe** en un cuaderno todas **aquellas cosas que has ido averiguando**.
6. **Escribe** también **cómo querrías que se solucionase** o terminase la situación.

7. **Si una vez analizada la situación sigues teniendo dudas** y no tienes quién te pueda ayudar a desvelarlas, o si consideras que lo que está ocurriendo es grave y no puedes ni asumirlo ni controlarlo, **habla** inmediatamente con tus padres.
8. Si crees que, por la escasa gravedad de la situación, por sus características, o incluso, por quien puede estar ofendiéndote (procura consultar con alguien de tu confianza) puedes afrontar los hechos y actuar para que se detengan inmediatamente, valora la posibilidad de hablar o tomar contacto con el compañero o compañeros causantes de la situación que te está afectando.
9. 9. En el caso de que la respuesta a tu intervención haya sido positiva y notes que se has sido entendido y se comprende tu queja, asegúrate de que los hechos que te han afectado dejan realmente de producirse y de que no quedan rastros significativos de los mismos. Exige que esto sea siempre así. Puedes buscar la ayuda de algún compañero en este proceso. Si es posible esta opción y la has llevado a cabo, escribe en tu cuaderno qué ha pasado y cómo te ha respondido.

   10. Si esta intervención no ha tenido éxito o tienes serias dudas sobre lo que puede pasar a partir de ese momento, pon en conocimiento de tus padres y/o profesores la situación en cuanto puedas. Pedir ayuda no es de cobardes. Todo lo contrario.

7.4 Protocolo de intervención del ciberacoso escolar

El artículo 124 de la **Ley Orgánica 3, de 29 de diciembre de 2020 de Mejora de la LOE**, en su punto 5 establece que las Administraciones educativas regularán los protocolos de actuación frente a indicios de acoso escolar, **ciberacoso**, acoso sexual, violencia de género y cualquier otra manifestación de violencia, así como los requisitos y las funciones que debe desempeñar **el coordinador o coordinadora de bienestar y protección**, que debe designarse en todos los centros educativos independientemente de su titularidad. **Las directoras, directores o titulares de centros educativos se responsabilizarán de que la comunidad educativa esté informada de los protocolos de actuación existentes, así como de la ejecución y el seguimiento de las actuaciones previstas en los mismos**. En todo caso deberán garantizarse los derechos de las personas afectadas.»



7.4.1 Fase I: Detección y obtención de información preliminar

Cualquier miembro de la comunidad educativa que tenga indicios y pruebas razonables de que puede estar produciéndose un caso de ciberacoso pondrá esta circunstancia en conocimiento de algún profesor, preferentemente el Tutor, Orientador o miembro del Equipo Directivo. Es imprescindible cuidar la confidencialidad y discreción en los procesos de comunicación. En cualquier caso, la información recibida deberá ponerse siempre en conocimiento del Equipo Directivo.

La información deberá ser analizada por el Equipo Directivo a la mayor brevedad con la colaboración del Tutor y del Orientador del Centro, así como también, del Inspector del Centro:

- Análisis de la información recibida, evidencias electrónicas y, en su caso, pruebas de la situación que ha sido puesta en conocimiento. Se entiende por evidencia electrónica cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad que prueba un hecho una vez realizado o bien que no ha sido realizado; por evidencia electrónica entendemos cualquier evidencia soportada en formato electrónico que permite archivar y reproducir la palabra, el sonido, la imagen y datos de cualquier otra clase.
- Determinación de alumnos implicados como presuntos agresores y víctimas. Valoración de antecedentes y posibles experiencias relacionales en espacios comunes, aulas, actividades complementarias y extraescolares.
- Valorar tanto la posibilidad de una entrevista con el alumno presuntamente objeto de maltrato como la de desarrollar un plan de entrevistas (según necesidad y pertinencia,

a compañeros, profesorado, familias de los alumnos implicados…). Todo ello en el marco de la más absoluta discreción y confidencialidad.

Ayudar a los alumnos a detectar y analizar las situaciones y a tomar las decisiones adecuadas. Es especialmente importante poder guiar la acción de nuestros alumnos en los casos que presuntamente puedan ser considerados como ciberacoso.

7.4.2 Fase II: La valoración del caso: indagación y primeras propuestas.

Con carácter preliminar, el Equipo Directivo analizará y valorará la situación a la luz de los datos y evidencias recabados de la información preliminar. De la citada valoración y según los indicios y pruebas con los que se cuenta, dependerá la adopción de medidas a planificar. Incluida la posibilidad de apertura de procedimientos disciplinarios y, en su caso, sancionadores, según lo establecido en el Reglamento de Régimen Interno y en la normativa vigente. La tasación de la situación es fundamental para configurar el itinerario a seguir en el proceso.

- Análisis de la información recibida, evidencias electrónicas y, en su caso, pruebas de la situación que ha sido puesta en conocimiento. Se entiende por evidencia electrónica cualquier dato o información que pueda ser utilizado para determinar o demostrar la veracidad que prueba un hecho una vez realizado o bien que no ha sido realizado; por evidencia electrónica entendemos cualquier evidencia soportada en formato electrónico que permite archivar y reproducir la palabra, el sonido, la imagen y datos de cualquier otra clase.

El Equipo Directivo ha de garantizar, a través de las intervenciones que se estimen pertinentes por parte del profesor o profesores que se designen, el adecuado proceso de acogida, cuidado, apoyo y escucha del alumno-víctima, aportándole seguridad y atención incondicional. Asimismo, resulta imprescindible que, sin perjuicio de las acciones de investigación a desarrollar, se pongan en marcha medidas que permitan evidenciar el cese del acoso. Puede ser de interés abordar la situación en el grupo o grupos-aula afectados o implicados, en el contexto de un proceso de reflexión y toma en consideración de lo acontecido, y de los pasos subsiguientes a poner en marcha por el centro.

La investigación contemplará las actuaciones a continuación detalladas.

7.4.2.1 Acciones de búsqueda de información

Los implicados (víctima y agresor o agresores): solicitud de información y obtención de referencias específicas de la situación detectada:

- **La entrevista con la víctima**. La entrevista con la víctima deberá contemplar la acogida de la misma, la valoración de los efectos y consecuencias producidos, la discreción y confidencialidad de las actuaciones, la posible identificación de los presuntos agresores y la imprescindible garantía de discreción y toma en consideración de lo

expuesto y del desarrollo de acciones que se estimen pertinentes en función de la valoración del caso.

- **La entrevista con el posible agresor o agresores**. Deberá contemplar la información sobre los hechos acontecidos y las evidencias encontradas, su valoración de los mismos, su actitud ante las consecuencias producidas y, de modo expreso, ante subsiguientes procesos de reparación del daño y reconciliación.

Las familias de los alumnos implicados (víctima y agresor o agresores):

- **Las entrevistas con la familia del alumno víctima** deberán incorporar cautelas que garanticen la actitud decidida hacia la intervención correctora en caso de que sea preciso, el ajuste a reglamento y la discreción dentro del proceso de investigación, así como la solicitud de colaboración para eventuales actuaciones subsiguientes tales como, el contacto con la familia del presunto agresor.
- **Las entrevistas con la familia del agresor o agresores** deberán cuidar especialmente la aportación ordenada de los datos recabados, la solicitud de colaboración en el proceso de valoración y toma de decisiones definidos, y el adecuado tratamiento de posibles respuestas de confrontación ante la situación planteada.

Entorno próximo:

- **Compañeros que puedan ser conocedores de la situación.** Las entrevistas con los compañeros posibles conocedores de la situación detectada deberán en todo caso recabar información y solicitar la colaboración imprescindible para detener el conflicto y reducir los efectos perniciosos producidos.
- **Los profesores de los alumnos afectados o implicados.** Es imprescindible recabar información y la colaboración de los profesores de los alumnos afectados o implicados.

La acción ordenada, adecuadamente documentada, secuenciada y planificada es una garantía para contar con la colaboración de todos aquellos (compañeros o profesores) que forman el contexto de relación de los alumnos implicados.

7.4.2.2 Informe

La información recabada deberá detallar lo más explícitamente posible los siguientes apartados:

- La naturaleza, intensidad y gravedad de los hechos.
- Alumnos implicados y afectados.
- Duración de la situación.
- Efectos producidos.
- Conocimiento de la situación por compañeros.
- Características de los medios y dispositivos utilizados.

Resulta imprescindible ordenar adecuadamente las actuaciones y garantizar la información a los implicados sobre el proceso desarrollado y la discreción en el tratamiento de los datos e información recabada.

7.4.2.3 Conclusiones

Se aportará información precisa y detallada del proceso a la Comisión de Convivencia del Centro y al/a la inspector/a del Centro.

7.4.2.4 Solicitud de asesoramiento.

La complejidad de este tipo de situaciones puede derivar en la necesidad de consulta y asesoramiento a Servicios externos al centro, según las circunstancias, necesidad y pertinencia. Entre otros, Agencia Española de Protección de Datos, Policía Local, Servicios Sociales o Unidades de Investigación Tecnológica o Delitos Telemáticos de las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil).

Para la valoración y tasación de una posible situación de ciberacoso, deberán tenerse en cuenta los siguientes aspectos:

- Características y naturaleza de las acciones analizadas y de los medios y dispositivos tecnológicos utilizados en la comisión de los hechos.
- Naturaleza y expansividad de la posible difusión de las acciones.
- Facilidad/Dificultad para detener el ciberacoso.
- Tiempo de exposición de la víctima al ciberacoso.
- Edad y características psicológicas de ésta y de los presuntos agresores.
- Repercusión e impacto en la víctima.

7.4.2.5 Adopción de medidas de carácter cautelar

En el supuesto de **confirmación de ciberacoso** entre iguales, podrán adoptarse medidas de naturaleza cautelar (Decreto 249/2007 modificado por Decreto 7/2019), informándose de las mismas al Tutor y Orientador, a la Comisión de Convivencia y a la Inspección Educativa. Asimismo, será comunicada con carácter previo a los padres o representantes legales de los alumnos.

- Adopción de medidas urgentes: el Equipo Directivo, con el conocimiento y asesoramiento del Orientador del Centro y del Servicio de Inspección Educativa, adoptará medidas de atención y apoyo al alumno objeto de maltrato: entre otras, tomar decisiones sobre procesos de ayuda y mejora de las condiciones personales, de interacción y habilidades sociales, así como del rendimiento escolar.
- Valoración sobre posibilidad de poner en conocimiento de Ministerio Fiscal o Fuerzas y Cuerpos de la Seguridad de Estado o locales.
- Cuando, tras la valoración de la situación detectada (naturaleza, características, intensidad y gravedad y efectos), no se derive una evaluación de ciberacoso, se tomará en consideración el desarrollo proporcionado de actuaciones que puedan incluir, respuestas de apoyo al alumno considerado víctima, rectificación y reparación de las acciones inadecuadas detectadas, comunicación a las familias y a la Comisión de Convivencia de la valoración efectuada y, de manera singular, el desarrollo de actividades didácticas de sensibilización, información y formación del alumnado.

Todas las actuaciones de investigación serán realizadas, dirigidas y orientadas por el Equipo Directivo del Centro y se detallarán en un Informe específico custodiado por el citado Equipo Directivo.

7.4.3 Fase III: plan de actuación, confirmación del ciberacoso

Son objetivos de esta tercera fase:

- El cese del ciberacoso.
- La protección, el cuidado y apoyo a la víctima.
- La reparación del daño causado, el perdón y la reconciliación.
- La sensibilización de la comunidad educativa.

Actuaciones con los alumnos afectados e implicados:

- Con la víctima: desarrollo de acciones de apoyo y protección, programas específicos de apoyo personal y social; derivación, si procede, a servicios externos.
- Con el agresor o agresores: desarrollo de programas de ayuda personal y social, pertinencia de aplicación del RRI y posible derivación a servicios externos.
- Con los compañeros: información básica; desarrollo de programas de favorecimiento de la convivencia pacífica y sensibilización.
- Actuaciones para la facilitar procesos de mediación entre víctima y agresor. Generar condiciones para la resolución del conflicto:
    - asunción de responsabilidades de los agresores.
    - reparación del daño.
    - perdón y reconciliación.

Todo ello a través de formatos de ayuda o mediación: con la participación de grupos de iguales, o a través de la acción tutorial, del equipo o departamento de Orientación, o de la Comisión de Convivencia. En el contexto de las actuaciones educativas, víctimas y agresores deben considerarse alumnos a los que acompañar en un proceso de ayuda, de diferente configuración, naturaleza y espectro, pero proceso de ayuda, en cualquier caso.

Actuaciones con las familias:

- Del alumno víctima: orientación sobre indicadores relevantes de comportamiento, pautas de atención y apoyo, seguimiento del caso, y orientación sobre posibles apoyos externos al centro.
- Del alumno agresor: orientación sobre indicadores relevantes de comportamiento, pautas de atención, apoyo y control de conductas, seguimiento del caso y orientación sobre posibles apoyos externos al centro.

Con el profesorado:

- Información.
- Sensibilización.
- Formación para la prevención y actuación en situaciones de ciberacoso y favorecimiento del desarrollo de patrones de convivencia pacífica.

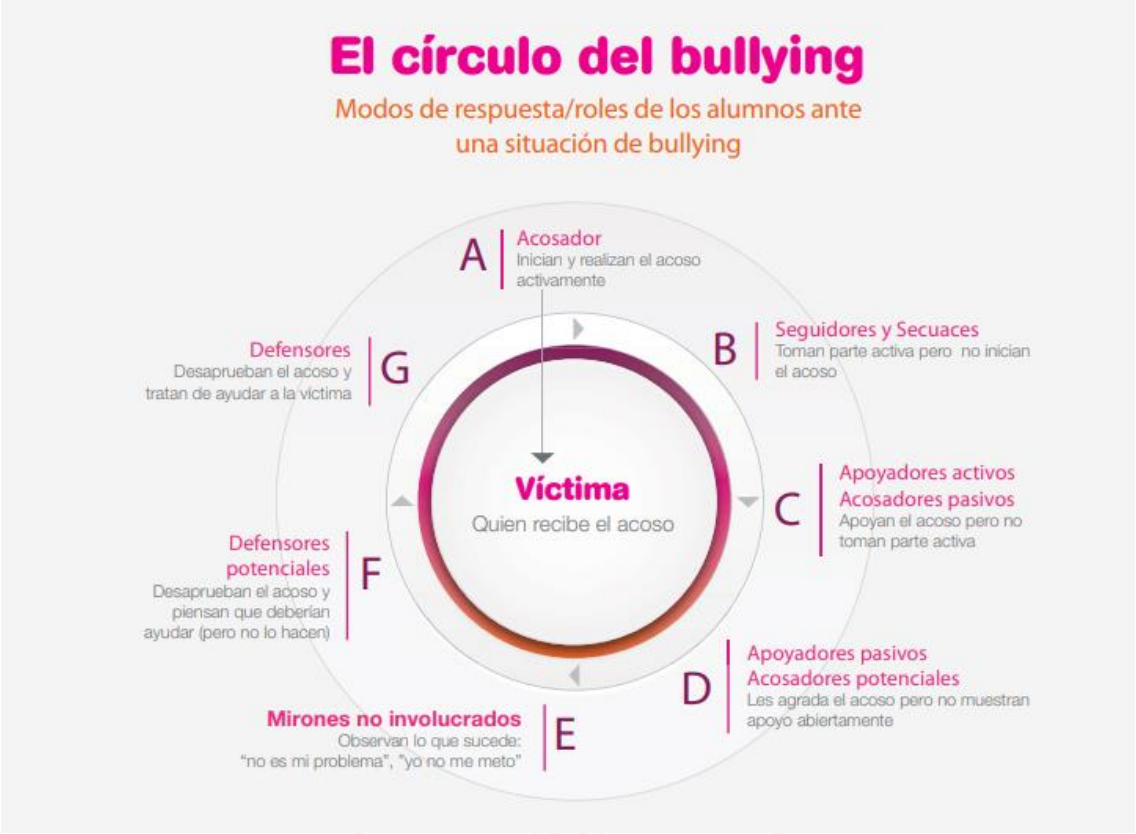
7.4.4 Fase IV: evaluación y seguimiento del plan

- Del caso concreto: resultados del plan en relación a la víctima y al agresor, situación de la víctima y del agresor, y actuaciones desarrolladas no previstas en el plan.
- De las actuaciones desarrolladas en el aula y en todo el centro.
- De las actuaciones de sensibilización y formación del profesorado.
- Del proceso de reflexión, análisis y sensibilización con las familias y el resto de la Comunidad Educativa.
- Del trabajo y actuaciones de la Comisión de Convivencia del Centro.

Todas las actuaciones llevadas a efecto en el proceso de seguimiento del Plan se recogerán en el Informe citado en las fases 2 y 3. Se aportará copia del Informe a la Comisión de Convivencia del Consejo Escolar del centro y al Servicio de Inspección Educativa.

7.4.5 Fase V: información y sensibilización. La necesidad de prevenir

El Equipo Directivo y la Comisión de Convivencia del Centro han de promover el diseño y desarrollo de actuaciones de información y sensibilización en la comunidad educativa en su conjunto. Esta es una tarea necesaria e imprescindible para informar y formar, para afrontar los retos desde la prevención. Conductas insolidarias, de abuso y dolor pueden servirnos de herramienta para la reflexión conjunta, para el análisis sosegado de lo que ha pasado, de por qué ha pasado, de los efectos que ha generado, de las soluciones planteadas y de las actuaciones desarrolladas. Aunque prevenir es imprescindible, la acción de sensibilización tras acontecimientos cercanos y hechos reales es singularmente efectiva.



Según la teorización de OLWEUS, a cuya obra se ha hecho referencia en la bibliografía del capítulo de Definición y Conceptualización del ciberacoso escolar.

8 Bibliografía

Panagiotis Kampylis, Yves Punie, Jim Devine. Promoción de un aprendizaje eficaz en la era digital. Un marco europeo para organizaciones educativas digitalmente competentes. 2015. Traducción: Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). Ministerio de Educación, Cultura y Deporte. España. 2016
https://sede.educacion.gob.es/publiventa/promocion-de-un-aprendizaje-eficaz-en-la-era-digital-un-marco-europeo-para-organizaciones-educativas-digitalmente-competentes/ensenanza-recursos-digitales/21199

El Plan Digital de Centro. Un marco para la integración de las tecnologías. Ministerio de Educación y Formación Profesional. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado
https://intef.es/Noticias/el-plan-digital-de-centro-un-marco-para-la-integracion-de-las-tecnologias/

Plan Digital de Centro. Descripción y guía. Ministerio de Educación y Formación Profesional. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado
https://intef.es/wp-content/uploads/2020/07/2020_0707_Plan-Digital-de-Centro_-INTEF.pdf

De Haro Ollé, Juan José. Ciudadanía e identidad digital. Ministerio de Educación y Formación Profesional. Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado. 2020
https://sede.educacion.gob.es/publiventa/ciudadania-e-identidad-digital/competencia-digital/24689

González, Edith. Formación Ciudadana [digital], una nueva materia para el currículum escolar. http://formacionib.org/noticias/?Formacion-Ciudadana-digital-una-nueva-materia-para-elcurriculum-escolar

Tourón, Javier. Transformación digital de la educación. 2021.
https://www.javiertouron.es/transformacion-digital-de-la-educacion/

Bermejo Fernández-Nieto, J. (1). Identidad digital. Retos para la función docente. Padres Y Maestros / Journal of Parents and Teachers, (370), 37-42.
https://doi.org/10.14422/pym.i370.y2017.006

Castañeda, L., & Camacho, M. (2012). Desvelando nuestra identidad digital. Profesional De La Información, 21(4), 354-360. https://doi.org/10.3145/epi.2012.jul.04

EMICI Equipo Multidisciplinar de Investigación sobre Ciberbullying. "**Protocolo de actuación ante el ciberbullying**". Gobierno Vasco.
http://www.protocolo-ciberbullying.com/

INTECO Instituto Nacional de Tecnologías de la Comunicación "Guía de actuación ante el ciberacoso". Ministerio de Industria, Turismo y Comercio.

Sánchez Pardo Lorenzo, Crespo Herrador Guillermo, Aguilar Moya Remedios (2013), Los adolescentes y el ciberacoso. Universidad de Valencia.

González-Cabrera Joaquín y varios (2017). Informe ejecutivo del proyecto Ciberastur. Universidad Internacional de La Rioja (UNIR).

Baquero Correa Abel y Avendaño Prieto Bertha (2015). "Diseño y análisis psicométrico de un instrumento para detectar presencia de cyberbullyng en un contexto escolar. Universidad de Colombia.

WILLARD, N (2007). "Cyber-Safe Kids, Cyber-Savvy Teens, Helping young people learn to use the Internet safely and responsibly". San Francisco (CA, USA): Jossey-Bass.

LI, Q. (2010). "Cyberbullying in High Schools: A Study of Students´ Behaviors and Beliefs about this new phenomenon" Journal of Aggression, Maltreatment and Trauma. Available at Tanfoline.

ORTEGA, R; ELIPE, P; MORA-MERCHÁN J; GENTA, M; BRIGHI, A; GUARINI, A; SMITH, P; THOMPSON, F Y TIPPETT, N:(2012) "The emotional impact of bullying and cyber-bullying on victims. A European Cross-National Study. En Aggressive Behaviour.

ZYCH, I; ORTEGA, R y MARÍN LÓPEZ, I (2016) "Cyberbullying AERA (American Educational Research Association) Prevention of bullying in Schools, Colleges and Universities" Washington DC (USA). American Educational Research Association.

CALMAESTRA, J; DEL REY, R; ORTEGA, R y MORA-MERCHÁN, J.A. (2012): "Introduction to cyberbullying".

HINDUYA, S y PATCHIN, J.W. (2009): "Bullying beyond the schoolyard. Preventing and responding to Cyberbullying". Thousand Oaks (CA, USA). Corwing Press.

HINDUYA, S y PATCHIN, J.W. (2010): "Cyberbullying and self-esteem" Journal of School Health.

OLWEUS, D. (2000): "Bullying at school". Oxford (U.K.). Blackwell.

SMITH, PK; MAHDAVI, J; CARVALHO, M; FISHER, S; RUSSELL, S y TIPPETT, N (2008): "Cyberbullying, its forms and impact on secondary school pupils". Journal of Child Psychology and Psychiatry.

KOWALSKI, RM; LIMBER, SP y AGATSON, PW (2008). "Cyberbullying. Bullying the Digital Age". Oxford (UK); Blackwell.

SOURANDER, A; BRUNSTEIN-KLOMEK, A; HELENIUS, H; IKONEN, M; LINDROOS, J; LUNTAMO, T y KOSKELAINEN, M (2010): "Psychological risk factors associated with cyberbullying among adolescents: A population based study. Archives of General Psychiatry.

VANDEBOSCH, H y CLEEMPUT, K (2009): "Cyberbullying among youngsters: profiles of bullies and victims". New Media & Society.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
https://www.boe.es/doue/2016/119/L00001-00088.pdf

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Informe sobre la utilización por parte de profesorado y alumnado de aplicaciones que almacenan datos en nube con sistemas ajenos a las plataformas educativas. Orientaciones para centros educativos. AEPD (Agencia Española de Protección de Datos)
https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-apps-datos-alumnos.pdf

Informe sobre uso de aplicaciones de dispositivos móviles y aplicaciones en la nube desarrollado por el Servicio de Inspección educativa.
https://www.educastur.es/-/informe-uso-de-apps-ajenas-a-plataforma-institucional-del-p-de-asturias

Guías sectoriales AEPD. Guía para centros educativos. Agencia Española de Protección de Datos (AEPD)
https://www.aepd.es/sites/default/files/2019-10/GuiaCentrosEducativos_.pdf

La protección de datos como garantía en las políticas de prevención del acoso: recomendaciones de la AEPD. Agencia Española de Protección de Datos (AEPD)
https://www.aepd.es/sites/default/files/2019-12/recomendaciones-sobre-acoso-digital-aepd.pdf

Protección del menor en Internet – Evita el contenido inapropiado preservando su privacidad. Agencia Española de Protección de Datos (AEPD)
https://www.aepd.es/sites/default/files/2020-04/nota-tecnica-proteccion-del-menor-en-internet.pdf

Mantener a los alumnos protegidos mientras usan Teams para el aprendizaje a distancia. Microsoft Teams para el ámbito educativo. Microsoft.com.
https://support.microsoft.com/es-es/topic/mantener-a-los-alumnos-protegidos-mientras-usan-teams-para-el-aprendizaje-a-distancia-f00fa399-0473-4d31-ab72-644c137e11c8?ui=es-es&rs=es-es&ad=es

9 Anexos

9.1 Crear un entorno seguro para el alumnado en Teams

En *Teams* pueden arbitrarse diferentes medidas y configuraciones que se consideran como recomendables para el ámbito educativo, tanto para administradores como para profesores. Estas medidas se conocen como *directivas de seguridad* y permite administrar las reuniones y los canales con los controles recomendados. Al trabajar en conjunto, estas configuraciones ayudan a garantizar un entorno más seguro y productivo para el alumnado.

Microsoft trabaja continuamente en la mejora de esta aplicación, por lo que los consejos y métodos descritos pueden variar y ampliarse. Puede encontrarse la información más reciente sobre este tema en la web de Microsoft:

Mantener a los alumnos protegidos mientras usan Teams para el aprendizaje a distancia - Soporte de Office (microsoft.com)

9.1.1 Por los administradores (Educastur)

Educastur, como administrador principal del entorno de Microsoft 365 para la comunidad educativa del Principado de Asturias, arbitra dos líneas de acción propias de su nivel de responsabilidad:

1. Creación y mantenimiento de identidades seguras para el alumnado y el profesorado.
2. Directivas de seguridad de Teams

9.1.1.1 Configurar identidades seguras para el alumnado y el profesorado

En el entorno Educastur el alumnado tiene una identidad digital que se concreta en el identificador único que le permite iniciar sesión en los diferentes servicios institucionales. Para los servicios de Microsoft 365, ese identificador único es seguido del dominio *@educastur.es*. En el caso del profesorado, ese identificador es seguido del dominio *@educastur.org*.

Identificarse para iniciar sesión en los servicios web es una forma de proteger a estos de entradas no autorizadas. Evitar el anonimato y, por tanto, que se pueda hacer trazabilidad de nuestras actuaciones, quedando la correspondiente autoría asociada a estas, es otro beneficio de la identidad digital. En el capítulo dedicado a la ciudadanía e identidad digital se aborda el trabajo de sensibilización y formación necesarios para su correcto uso.

9.1.1.2 Directivas de seguridad de Teams

Las directivas de Teams permiten definir cómo se comporta esta aplicación en Educastur y qué nivel de acceso tiene cada usuario individual a determinadas características. Para mantener la seguridad del alumnado, Educastur implementa ciertas directivas administrativas de forma que se puede controlar quiénes pueden hacer uso de ciertas funcionalidades y cómo usarlas en el caso de que sean permitidas.

Se han aplicado directivas de seguridad a las funcionalidades de mensajería y reunión para el alumnado:

Mensajería (Chat) e intervenciones en canales

- Los propietarios de los mensajes no pueden eliminar ni editar los mensajes enviados.
- Siempre se confirma la lectura de los mensajes.
- Se han desactivado los mensajes urgentes.
- Se han desactivado las imágenes Giphy, memes y adhesivos.
- El alumnado solo puede chatear con alumnado que esté en equipos comunes. No puede chatear con otro alumnado del propio centro o de otro si no tienen un equipo en común.
- El alumnado no puede ni eliminar ni modificar los mensajes. Esta directiva es de orden superior a la que especifique el profesorado en los Teams de clase que cree.

Reuniones

- No pueden hacer uso de la opción "Reunirse ahora" o programar reuniones de canal en los equipos creados por el profesorado.
- No se permite la grabación en la nube.

Buscar

- El alumnado solo puede buscar a usuarios que pertenezcan a equipos comunes.

9.1.2 Por el profesorado

El profesorado puede y debe supervisar la actividad y la comunicación que su alumnado desarrolla dentro de la aplicación. Se ofrecen muchas formas de ayudar al profesorado en la administración de la clase, por ejemplo, silenciando al alumnado que agregue mensajes que distraigan o que no sean adecuados para discusiones de grupo, y también eliminando los mensajes inadecuados. Hay que tener en cuenta que las directivas de primer nivel definidas por Educastur pueden condicionar las especificadas por el profesorado.

9.1.2.1 *Utilizar la versión más reciente de Teams*

Tener la última versión de la aplicación es básico para garantizar la máxima protección al alumnado y al propio profesorado. Si el alumnado usa dispositivos móviles para asistir a las reuniones, se les debe pedir que busquen las actualizaciones de forma periódica en la App Store de iOS o en Google Play Store.

9.1.2.2 *Crear una reunión segura y controlada para una clase*

Antes de la reunión

- Es recomendable programar las reuniones para la clase en los canales. Los canales permiten controlar mejor las reuniones al ofrecerle la opción de deshabilitar el chat entre el alumnado, por ejemplo.
- Como organizador de la reunión, debe administrar las opciones de la reunión antes de reunirse para aumentar la seguridad en línea del alumnado.
- Use las opciones de omitir la sala de espera de la reunión para controlar quién puede acceder directamente a la reunión sin necesidad de ser previamente admitido desde la

sala de espera. Limitar esta funcionalidad le ayudará a impedir que los usuarios no autorizados puedan acceder a sus reuniones.

- El moderador controla y administra las reuniones. En muchos casos es más seguro que el alumnado se una a las reuniones como asistente. De esta forma no puedan quitar a otros participantes o silenciarlos, y no tienen acceso a otros controles de reunión elevados. Con el rol de asistente, los alumnos aún podrán compartir vídeos, participar en el chat y ver los archivos compartidos en la reunión.
- De igual manera, podemos definir que el alumnado acceda a la reunión silenciado y que precisen del docente o de un moderador para poder activar el sonido.
- Se puede controlar cuándo está habilitado el chat de la reunión, bien haciendo que sea de solo lectura de forma que nadie pueda enviar mensajes en el chat, incluido el organizador. Esto evita que los chats se envíen antes, durante y después de la reunión. También se puede establecer que el chat se use solo en la reunión para permitir que los participantes solo envíen mensajes durante la reunión y que los organizadores puedan enviar mensajes en cualquier momento.
- Al inicio de la reunión, revise cuidadosamente la lista de participantes en la sala de espera y solo admita a los alumnos e invitados que considere autorizados a unirse a la reunión.

Durante la reunión

- Silenciar al alumnado permite minimizar las distracciones.
- Las opciones anteriores definidas antes de la reunión también pueden establecerse en el transcurso de esta.
- Los roles de moderador y asistente también pueden alternarse en el momento de reunirse si se precisa que el alumnado puntualmente pueda presentar contenido.

Después de la reunión

- Es conveniente asegurarse de que el alumnado deje la reunión seleccionando como profesorado Finalizar la reunión haciendo clic en esta opción que se esconde en *Más opciones* en los controles de la reunión. Esto hará que finalice la reunión para todos los participantes. Solo colgar la llamada o cerrar la ventana de la reunión no obliga al alumnado a salir de la reunión. El alumnado aún podrá ver el historial de chats.

9.1.2.3 Crear canales y equipos seguros para la clase

- Dentro de un canal, se pueden bloquear las respuestas del alumnado en una conversación específica. Esto permite al profesorado publicar mensajes en el canal, pero el alumnado no podrá agregar mensajes nuevos.
- El profesorado puede habilitar la moderación para un canal del equipo de clase y así controlar quién puede iniciar nuevas publicaciones y responder a las publicaciones de ese canal.
- Si un alumno de un canal del equipo está interrumpiendo la clase, se le puede silenciar por un tiempo determinado a través de la configuración del equipo.
- Por último, se puede controlar quien puede *@mencionar* al equipo y si el alumnado puede usar imágenes de *Giphy*, adhesivos o memes.