LA EDUCACIÓN EN PRIMER LUGAR

Orientaciones para uso de plataformas y trabajo virtual de la comunidad educativa

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Orientaciones para uso de plataformas y trabajo virtual de la comunidad educativa

Recomendaciones para promover prácticas de aprendizaje seguro en la virtualidad y diseñar protocolos de uso de plataformas.

El presente documento corresponde a la primera versión de las recomendaciones para promover prácticas de aprendizaje seguro en la virtualidad y diseñar protocolos de uso de plataformas para la Secretaría de Educación del Distrito, el mismo puede estar sujeto a actualizaciones y ajustes para su mejoramiento a futuro.

Versión 1, septiembre de 2020.

Secretaría de Educación Distrital
Edna Bonilla Sebá

Subsecretaría de Calidad y Pertinencia
Andrés Mauricio Castillo Varela

Subsecretaría de Integración Interinstitucional
Deidamia García

Oficina de Servicios Administrativos RedP
Wilson Adiel Rodríguez Rodríguez

Dirección de Ciencias, Tecnologías y Medios Educativos
Ulia N. Yemail Cortés

Dirección de Participación y Relaciones Interinstitucionales
Edwin Alberto Ussa Cristiano

Equipo técnico
Jonathan Andrés Sánchez Corredor
José Miguel Home Rodríguez
Patricia Niño Rodríguez
Dirección de Ciencias, Tecnologías y Medios Educativos

Andrés Felipe Avendaño Herrera
Dirección de Participación y Relaciones Interinstitucionales

Henry Alexander Moyan Montenegro
Oficina de Servicios Administrativos RedP

Navegar y aprender de forma segura es compromiso de todos

Las medidas adoptadas por los Gobiernos nacional y distrital a propósito de la pandemia de coronavirus (COVID-19), nos ha exigido, desde el sector educativo el diseño e implementación de prácticas de enseñanza y aprendizaje flexibles, mediadas por tecnologías de la información y la comunicación TIC.

Para apoyar este proceso la Secretaría de Educación del Distrito (SED) ha puesto en marcha la estrategia "Aprende en Casa", la cual buscar brindar orientaciones y acompañamiento a los diferentes actores de la comunidad educativa para la generación de prácticas y estrategias de flexibilización escolar, que garanticen que los niños, niñas, adolescentes y jóvenes puedan continuar su proceso de aprendizaje desde el hogar. Uno de los elementos clave ha sido poner a disposición canales y medios de comunicación virtuales, para ser utilizados por directivos docentes, docentes, administrativos y estudiantes.

El uso de estas herramientas implica un reto pedagógico y de seguridad, pues el uso responsable y seguro es una tarea de todos, por eso, este documento tiene por objetivo aclarar cuáles son las herramientas virtuales habilitadas por la SED para posibilitar procesos pedagógicos, comunicativos, administrativos y brindar orientaciones para el diseño de protocolos, rutas de atención y recomendaciones para la protección de los estudiantes.

Estas orientaciones son una base que debe enriquecerse con la construcción colectiva que se desarrolle en cada institución educativa, un proceso mediado por la participación de estudiantes, padres de familia y que debe promover procesos de formación y desarrollo de la ciudadanía digital, basados en la responsabilidad, la autonomía y el autocuidado.

1 Herramientas tecnológicas para el desarrollo de actividades pedagógicas

La SED de manera permanente trabaja en el fortalecimiento de la infraestructura tecnológica y de los servicios que se ofrecen a la comunidad educativa y en particular a los colegios del distrito, con el fin de apoyar de manera pertinente el desarrollo de las actividades educativas. Esto permite contar con un ecosistema tecnológico con plataformas estables y robustas que son monitoreadas y soportadas por un equipo de seguridad de la información, lo que reduce riesgos de tipo cibernético para docentes, directivos y especialmente, estudiantes.

Por lo anterior, desde la SED y respetando la autonomía institucional, se prioriza y promueve el uso de dichas plataformas, sobre las cuales, además, se desarrollan procesos de formación para lograr su máximo aprovechamiento.

A continuación, se describen las plataformas tecnológicas oficiales que la SED ha puesto a disposición para el desarrollo de actividades educativas:

1.1. *Office 365:* encontrarnos, compartir y participar

El acceso a las plataformas de Office 365 se realiza por medio de los correos institucionales de administrativos, directivos docentes, docentes y estudiantes. Cabe aclarar que toda la comunidad educativa distrital, cuenta con este beneficio, solo debe activar su correo electrónico institucional.

La creación de un correo electrónico institucional se hace a través del siguiente proceso:

Creación de correo electrónico para docentes:

La responsabilidad de la creación de los correos de docentes está a cargo del rector del colegio, para ello deberá diligenciar el "Formato de reporte de novedades para acceso a medios de procesamiento de información (adjunto al protocolo)", en dicho formato se encuentra el instructivo de diligenciamiento.

Tener en cuenta:

- ***Para la creación de cuenta de correo electrónico de solo un (1) docente:*** diligenciar pestaña "Formato solicitud Individual" según instructivo.

- ***Para la creación de cuentas de correo de dos (2) o más docentes:*** diligenciar pestaña **"Formato solicitud Individual"** con los datos del rector y pestaña "**Creación cuentas masivas"** con los datos de los docentes según instructivo.

  Nota: el formato no podrá ser modificado y debe ser diligenciado en mayúsculas.

  Enviar el formato debidamente diligenciado desde el correo institucional del colegio a la cuenta de correo de la Mesa de Servicios TIC de la SED: soportesed@educacionbogota.edu.co

- Restablecer contraseñas de correo institucional docentes:

- Para restablecer contraseñas de correo de los docentes se deberá enviar la solicitud a la Mesa de Servicios TIC de la entidad: soportesed@educacionbogota.edu.co desde un correo institucional (del colegio o compañero de trabajo) indicando: la cuenta de correo a la que se le debe restablecer contraseña, nombres completos del docente que requiere el servicio, cédula, colegio y número de teléfono.

Creación de correo electrónico para estudiantes:

La responsabilidad de la creación de los correos para estudiantes está a cargo del rector del colegio, para ello deberá diligenciar el "Formato de reporte de novedades para acceso a medios de procesamiento de información (adjunto al protocolo)", en dicho formato se encuentra el instructivo de diligenciamiento. Para ello se debe tener en cuenta:

- Para la creación de cuentas de correo masivas de estudiantes se deberá diligenciar pestaña "Formato solicitud Individual" con los datos del rector y pestaña "Creación cuentas masivas" con los datos de los estudiantes de la institución según indicaciones del formato.

  Nota: el formato no podrá ser modificado, solo se debe ingresar la información requerida y bajo los parámetros establecidos en el mismo, debe ser diligenciado en mayúsculas y se debe enviar un solo formato por todos los estudiantes de la institución, no por jornada, curso, etc.

Enviar el formato debidamente diligenciado desde el correo institucional del colegio a la Mesa de Servicios TIC de la entidad: soportesed@educacionbogota.edu.co

Herramienta	Descripción
Microsoft Teams	Corresponde a una plataforma unificada de comunicación y colaboración que combina chat, reuniones de video, almacenamiento de archivos e integración de aplicaciones. Cartilla que describe la herramienta: *https://www.redacademica.edu.co/catalogo/cartilla-teams* Manuales de usuario para administrativos, directivos docentes y docentes: *https://www.redacademica.edu.co/catalogo/microsoft-teams-para-usos-educativos* Seleccionar en para más información "Microsoft: ver manuales de uso"
One Drive	Servicio de alojamiento de archivos, en el cual puede compartir documentos para trabajo colaborativo en línea.
Forms	Es un creador de encuestas en línea, el cual permite adquirir información de la comunidad educativa.
SharePoint	Es una plataforma de colaboración basada en el navegador web, módulos de administración de procesos, módulos de búsquedas y un módulo para gestión documental.

Para saber más del uso de Office 365
Puede consultar los talleres de uso realizados en "Aprende en Casa con Saber Digital":***https://www.redacademica.edu.co/catalogo/especiales/diferidos-microsoft-teams***

1.2. Red Académica: el portal educativo para articularnos

A través del Portal Educativo Red Académica, la comunidad educativa tiene acceso a servicios de Portal Web Escolar y aulas virtuales Moodle, además, de un conjunto de más de 800 contenidos educativos digitales y una agenda de actividades digitales de carácter formativo, en temas como lectura y escritura, bilingüismo y uso de herramientas digitales, entre otros.

Herramienta	Descripción
Portal Web Escolar	Servicio de portal web para comunicación con la comunidad educativa. Los colegios en su portal pueden anexar elementos descriptivos (logo, misión, visión, datos de contacto, etc), vincular las redes sociales institucionales, publicar noticias para la comunidad educativa, agregar documentos institucionales, anexar una agenda de programación y vincular contenidos en formato multimedia. La información para solicitud del portal y la administración del mismo puede ser consultada en el link: *https://www.redacademica.edu.co/catalogo/qu-es-un-portal-web-escolar*
LMS Moodle Aulas Virtuales	Es un sistema de gestión de aprendizaje, en el cual las instituciones educativas pueden crear y dinamizar aulas virtuales. EL proceso de solicitud de aulas puede consultarse en: *https://www.redacademica.edu.co/catalogo/cartilla-moodle*

Para saber más del uso Portales Web y Aulas Virtuales
Puede consultar los talleres de uso realizados en "Aprende en Casa con Saber Digital": ***https://www.redacademica.edu.co/catalogo/especiales/diferidos-portal-web-escolar***

2 Orientaciones para la elaboración de protocolos para el trabajo en medios virtuales

Teniendo en cuenta la autonomía institucional, se sugiere a cada colegio la elaboración de protocolos de uso de las plataformas digitales. Para esto, se recomienda la conformación de un Equipo TIC, un grupo de profesionales con experiencia en temas digitales, con representantes de padres y estudiantes que puedan revisar y articular las indicaciones de la SED, las condiciones institucionales, las premisas de los procesos pedagógicos que se están desarrollando y las indicaciones ya previstas en el manual de convivencia y que es necesario incorporar y anticipar en estos protocolos.

Para orientar esta elaboración, consideramos pertinente tener en cuenta:

1. Documentarse sobre los alcances de cada plataforma

Como se ha mencionado en el apartado anterior, la SED dispone de un ecosistema tecnológico con plataformas estables y robustas que son monitoreadas y soportadas por un equipo de seguridad de la información, lo que reduce riesgos de tipo cibernéticos para docentes, directivos y especialmente, estudiantes.

Para conocer, más sobre ellas puede consultar:

Edusitio LabTic

Un espacio para el fortalecimiento de capacidades en el uso de TIC, en el cual se encuentran herramientas y contenidos que facilitan la adopción y apropiación de diferentes soluciones digitales, así como recomendaciones para el uso seguro de Internet.

https://www.redacademica.edu.co/estrategias/saber-digital/labtic

Manuales de uso

a. De Microsoft Teams
https://www.redacademica.edu.co/catalogo/microsoft-teams-para-usos-educativos

- Seleccionar en para más información “Microsoft: ver manuales de uso”

b. De Portal Web Escolar
https://www.redacademica.edu.co/catalogo/qu-es-un-portal-web-escolar

c. De Aulas Virtuales - LMS Moodle
https://www.redacademica.edu.co/catalogo/cartilla-moodle

2. Tener en cuenta consideraciones básicas generales

- Para el trabajo con estudiantes menores de edad, se debe gestionar la autorización de uso de imagen y grabaciones con los padres, madres o adultos acudientes. La SED sugiere el **"Formato para uso de imagen".**
- Para la programación de una reunión, clase o encuentro es importante conocer con anticipación las opciones de seguridad que ofrece la plataforma Teams y configurar las mismas. Para esto puede consultar **"Manual de seguridad Teams".**
- Cada vez que se programe un encuentro virtual es necesario explicitar la finalidad del mismo: clase de ____, temas a tratar_____
- El ingreso de cada participante debe ser individual y personal. Por esto, hay que, en una sesión previa con padres y estudiante, aclarar las implicaciones de la suplantación.
- El encargado de la reunión, clase o convocatoria no puede permitir el acceso de personas que no estén claramente identificadas y no sean parte del grupo de convocados.
- El estudiante o asistente, debe ingresar al aula virtual o reunión, identificándose con el nombre y apellido, acompañado del grado que cursa. No se debe permitir el uso de alias o apodos. Ejemplo: Pedro Gómez 802.
- Se recomienda por temas de seguridad de la información, que los ingresos se realicen a través de las cuentas oficiales establecidas por la SED.
- Se debe solicitar a los estudiantes o asistentes tener las cámaras y micrófonos apagados, solo encenderlos cuando sea requerido por el profesor o quien dirige la charla. En el caso de los estudiantes, si se solicita el uso de la cámara se debe contar con la autorización previa de los padres o acudientes.

- Se debe informar, previamente, que no se puede realizar, publicar o transmitir archivos que contengan contenido pornográfico, obsceno o difamatorio y las consecuencias de esta conducta.

- Los padres de familia o acudientes, pueden ser acompañantes de las actividades más no participantes activos de la clase, a menos que estos sea parte integral de la clase preparada. Esto debe informarse con anterioridad.

- Si el equipo de cómputo, celular o dispositivo no cuenta con cámara, esta situación no puede ser impedimento para ingresar al aula virtual.

Tips de seguridad

- Para las cuentas de correo electrónico oficiales, se deben utilizar contraseñas seguras, es decir, que tengan ocho o más caracteres e incluyan mayúsculas, minúsculas, números y caracteres especiales.

- Evitar acceder a las plataformas ofrecidas desde equipos públicos.

- No ejecutar los archivos adjuntos que provengan de remitentes desconocidos en los casos de correos electrónicos.

- Evitar hacer clic en los enlaces desconocidos o direcciones no confiables.

- No proporcionar datos como contraseñas personales o cualquier tipo de dato sensible durante el chat, reunión o el intercambio de correos electrónicos.

3. Estar atentos y anticipar posibles situaciones de vulneración de derechos

En las interacciones en espacios virtuales se pueden presentar situaciones de vulneración de derechos de los participantes que pueden obedecer a dos tipos:

a. Por alteraciones de seguridad de información en la plataforma Microsoft Teams.

Cuando esta ocurra, se debe remitir un oficio a la Oficina de Servicios Administrativos REDP desde donde guiarán el proceso a seguir con su equipo de seguridad de la información.

b. Por situaciones de maltrato o vulneración de derechos, catalogados como ciberacoso.

Cuando esto ocurra, es importante tener en cuenta las siguientes recomendaciones hechas por el Ministerio de Tecnologías de la Información y las Comunicaciones.

1. Evite contestar a las provocaciones, el hecho de contestar suele ocasionar que el ataque se recrudezca.

2. Pida ayuda y recuérdele a los niños, niñas, adolescentes y jóvenes de su entorno que lo mejor es acudir a usted en caso de atravesar por una circunstancia de este tipo.

3. Guarde las conversaciones, los mensajes y los contenidos que hagan parte de la agresión. Esto servirá de evidencia para reportar y denunciar el caso.

4. Reporte o denuncie la situación ante las autoridades, puede hacerlo a través del canal de reporte http://teprotejo.org/, dedicado a atender situaciones con menores de 18 años, o al CAI virtual https://www.policia.gov.co/

Para saber más
Consulte el portal *web www.enticconfio.gov.co/ del MinTIC.*

[1].https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/125828:Cinco-tips-para-afrontar-el-ciberacoso

3 Tips para la protección de niñas, niños, adolescentes y jóvenes y promover el uso responsable de redes sociales y medios tecnológicos

Actualmente, los estudiantes y sus familias están haciendo uso de múltiples soportes tecnológicos y medios de acceso (computadoras, tabletas, etc.), por lo cual se hace necesario informar y formar a la comunidad educativa frente a cómo realizar un uso adecuado de estas herramientas y qué riesgos se pueden tener en dichos espacios.

Para esto, es importante estar atentos e identificar algunas situaciones que se pueden presentar por medios electrónicos y a las cuales niños, niñas, adolescentes y jóvenes se encuentran expuestos. Las más comunes son:

Situación	Descripción
Grooming	Es una forma de acoso sexual que ocurre principalmente por medio de chats y redes sociales. Por medio de una conversación virtual, el acosador puede hacerse pasar por otra persona, con el fin de obtener satisfacción sexual mediante imágenes eróticas o pornográficas o propuestas relacionadas.
Sexting	Es el intercambio de fotos propias de contenido sugestivo o sexualmente explícito, las cuales se envían a otras personas vía teléfono celular o Internet.
Phishing	Método más utilizado por cibercriminales para estafar y obtener información confidencial de forma fraudulenta.
Ciberacoso Cyberbullying	Acto agresivo e intencionado que se lleva a cabo de manera repetida y constante a lo largo del tiempo mediante contacto electrónico, por parte de un grupo o de un individuo contra una víctima que no puede defenderse fácilmente, pues no hay donde esconderse, no se puede controlar la amplitud de la audiencia y puede haber invisibilidad de los acosadores.
Sextorsión	Aunque puede llegar a estar muy relacionado, cabe no confundir este término con el sexting. La sextorsión se trata de chantaje sexual. El extorsionador chantajea a la víctima con contenido privado del usuario, normalmente fotos o vídeos sexualmente explícitos. Este contenido puede ser conseguido mediante el hackeo de aparatos tecnológicos, el sexting o el grooming. A cambio de no difundir dicho contenido los delincuentes exigen algo a cambio, desde dinero, más contenido, pagos o favores de índole sexual.

Para saber más

Consulte las charlas de Internet seguro, disponibles en "Aprende en Casa con Saber Digital" ***https://www.redacademica.edu.co/catalogo/especiales/diferidos-intenet-seguro***

Recomendaciones para uso de redes sociales

Las redes sociales son ahora parte de nuestra cotidianidad. Estas entretienen y ahora educan, por lo cual es importante que su uso esté mediado por recomendaciones, reglas de uso y acompañamiento de padres y adultos cuidadores.

Algunas recomendaciones básicas, para tener en cuenta son:

- Pensar muy bien qué imágenes, videos e información se publican. Una vez en la red son públicas y es difícil controlar su divulgación.
- No publicar nunca información privada (dirección, teléfono o fotos donde se evidencien estos datos).
- Configurar cuentas y publicaciones en modo privado.
- No guardar contraseñas de forma automática cuando se usen equipos públicos.
- No aceptar solicitudes de amistad, links o invitaciones de personas desconocidas. Verificar todos los contactos.
- No dar información privada a personas por medio de las redes sociales.
- Verificar cualquier situación en la cual se solicite información privada o se invite a interacciones personales. Pueden ser estafas.
- Al registrarse en una red social o grupo virtual, usar la dirección de correo institucional con el fin de verificar tu cuenta.

Cuidados frente a lo académico y lo personal

- Tener cuidado de cómo se representa en Internet el establecimiento educativo o a los compañeros de aula. Hay que aclarar que no se deben publicar fotos de terceros sin la debida autorización.
- No mezclar el ámbito académico con el personal, en lo posible se debe evitar el relacionamiento por redes privadas entre estudiantes y docentes o administrativos.
- Realizar las configuraciones de privacidad pertinentes para la consulta de información de perfil.
- Permitir a padres de familia vincularse a grupos académicos con el fin de ser veedores de la información que se intercambia por estos espacios.
- No compartir usuarios y contraseñas, estos pueden ser usados para realizar actos que pueden ocasionar problemas académicos, convivenciales y en casos críticos, penales.
- Configuraciones de privacidad de cuentas de correo y redes sociales
- Usar opciones orientadas a la privacidad (comprobar quién puede ver las fotos publicadas, quién puede ponerse en contacto con nosotros y quién puede añadir comentarios).
- Informar inmediatamente casos de robo o pérdida del teléfono celular.
- Si le contactan de números extraños o correos desconocidos es necesario solicitar la identificación adecuada antes de dialogar con la persona.
- Los padres y adultos cuidadores deben revisar con regularidad el celular de los estudiantes, teniendo en cuenta que el uso de redes sociales se aconseja luego de los 13 años.
- Estar atento a identificar y bloquear personas con contenidos inapropiados.

Posibles delitos que se pueden cometer, sin tener intención de hacerlo

- Compartir fotos íntimas de terceros. La información de contenido íntimo no puede ser compartida sin autorización, puesto que esto es catalogado como un delito informático.

- Cualquier contenido de menores de edad que sea compartido a terceros se convierte en un delito informático al compartir datos sensibles y privados sin autorización previa y pueden comprometer o poner en riesgo la vida o integridad de un menor de edad.

- El acoso o la discriminación tanto en espacios físicos como virtuales son considerados delitos que atentan contra la identidad de las personas.
- El suplantar a un ciudadano en forma física o electrónica es un delito y acarrea un proceso penal.

- La violencia sexual también se expresa de forma de hostigamiento e intimidación, lo cual no está exento en espacios electrónicos, y también es catalogado como un delito.

4 ¿Cómo actuar en caso de evidenciar algún tipo de violencia o vulneración en la virtualidad?

En caso de ser víctima de algún evento de los mencionados en el apartado anterior, se debe realizar la activación de los protocolos de atención para situaciones de presunta agresión y acoso escolar y el protocolo de atención para situaciones de presunta violencia sexual, según corresponda, los cuales pueden ser encontrados en el "Directorio de protocolos de atención integral para la convivencia escolar y el ejercicio de los derechos humanos, sexuales y reproductivos", accediendo a través del siguiente enlace de la página web de la SED: ***https://www.educacionbogota.edu.co/portal_institucional/gestio-educativa/atencion-y-seguimiento.***

Así las cosas, la SED viene liderando desde 2016, en el marco del Comité Distrital de Convivencia Escolar (CDCE), la revisión, ajuste, aprobación y divulgación de los protocolos de atención integral para la convivencia escolar y el ejercicio de los derechos humanos, sexuales y reproductivos, que hacen parte de la Ruta de Atención Integral definida en la Ley 1620 de 2013 y su Decreto reglamentario 1965, del mismo año. Dentro del conjunto de los 17 protocolos, se cuentan con varios para el abordaje y atención de situaciones de violencias basadas en género.

Así mismo, es importante mencionar que la SED viene trabajando arduamente en el cumplimiento de la Ley 1620, trabajando de manera conjunta con la comunidad educativa del distrito, velando así por el fortalecimiento de la convivencia escolar, a través del uso e implementación de los protocolos de atención por parte de todos los colegios, así como el uso de la plataforma del Sistema de Alertas, estipulada en esta Ley como el Sistema Unificado de Información. Dicha plataforma, es usada para el reporte de situaciones de vulneración por parte de establecimientos educativos distritales y privados, generando así información de gran utilidad para el abordaje y gestión de situaciones en contra de niñas, niños y adolescentes.

En este orden de ideas, los protocolos contienen un conjunto de actividades, pautas y orientaciones que deben seguir los establecimientos educativos en el Distrito cuando identifiquen o tengan conocimiento de una presunta situación que afecte la convivencia escolar y vulnere los derechos humanos, sexuales y reproductivos de los estudiantes. Igualmente contempla acciones para la articulación con las entidades del orden distrital o nacional que tienen competencia en procesos de atención integral y de restablecimiento de derechos, así como acciones para realizar los seguimientos correspondientes.

A continuación, se relacionan los protocolos de atención, que hacen parte del "Directorio de protocolos de atención integral para la convivencia escolar y el ejercicio de los derechos humanos, sexuales y reproductivos", que se han venido actualizando desde el año 2014.

1. Protocolo de atención para presuntas situaciones de incumplimiento, negligencia y/o abandono de las responsabilidades de padres, madres y cuidadores.
2. Protocolo de atención para situaciones de presunto trabajo infantil o en riesgo de estarlo.
3. Protocolo de atención para situaciones de conducta suicida.
4. Protocolo de atención para situaciones de conducta suicida no fatal en niños, niñas y adolescentes (ideación, amenaza o intento).
5. Protocolo de atención para situaciones de presunto suicidio consumado.
6. Protocolo de atención para situaciones de presunta violencia sexual.
7. Protocolo de atención para situaciones de presunta agresión y acoso escolar.
8. Protocolo de atención para situaciones de embarazo adolescente, paternidad y/o maternidad temprana.
9. Protocolo de atención para situaciones de presunta violencia intrafamiliar.
10. Protocolo de atención para situaciones de presuntos casos que competen al sistema de responsabilidad penal para adolescentes (SRPA).
11. Protocolo de atención de niños, niñas y adolescentes con presunto consumo de sustancias psicoactivas (SPA).
12. Protocolo de atención para situaciones de presunta violencia contra niñas, adolescentes y mujeres por razones de género.
13. Protocolo de atención para situaciones de hostigamiento y discriminación por orientaciones sexuales, identidades y expresiones de género diversas.
14. Protocolo de atención para situaciones de presunto racismo y discriminación étnico – racial.

15. Protocolo de atención de niños, niñas y adolescentes víctimas y afectados por el conflicto armado residentes en Bogotá.

16. Protocolo de atención para la prevención del reclutamiento forzado de niños, niñas y adolescentes en Bogotá.

17. Protocolo de atención de siniestros viales para establecimientos educativos del distrito capital.

Par efectos de estas orientaciones, a continuación, se describe el protocolo de agresión y acoso escolar.

Definición de agresión o acoso escolar

- ***Agresión escolar.*** "Es toda acción realizada por uno o varios integrantes de la comunidad educativa y que busca afectar negativamente a otras personas de la misma comunidad, de las cuales por lo menos una es estudiante" (MEN, 2013, artículo 39). La agresión escolar puede ser:

- ***Física.*** Toda acción que tenga como finalidad causar daño al cuerpo o a la salud de otra persona. Incluye puñetazos, patadas, empujones, cachetadas, mordiscos, rasguños, pellizcos, jalón de pelo, entre otras.

- ***Verbal.*** Toda acción que busque con las palabras degradar, humillar, atemorizar o descalificar a otras personas. Incluye insultos, apodos ofensivos, burlas y amenazas.

- ***Gestual.*** Toda acción que busque con los gestos degradar, humillar, atemorizar o descalificar a otros.

- ***Relacional.*** Toda acción que busque afectar negativamente las relaciones que otros tienen. Incluye excluir de grupos, aislar deliberadamente y difundir rumores o secretos buscando afectar negativamente el estatus o imagen que tiene la persona frente a otros.

- ***Electrónica.*** Toda acción que busque afectar negativamente a otras personas a través de medios electrónicos. Incluye la divulgación de fotos o videos íntimos o humillantes en Internet, realizar comentarios insultantes u ofensivos sobre otros a través de redes sociales y enviar correos electrónicos o mensajes de texto insultantes u ofensivos; tanto de manera anónima como cuando se revela la identidad de quien los envía.

- ***Esporádica.*** Cualquier tipo de agresión que ocurre solo una vez, es decir, que no hace parte de un patrón de agresiones repetidas contra una misma persona. Este concepto incluye eventos aislados de agresión física, verbal o relacional. No incluye agresiones electrónicas que se realizan en redes sociales virtuales, dado que estas, al divulgarse, se convierten en ofensas repetidas. Por ejemplo, subir una foto íntima a una red social en Internet no puede considerarse agresión esporádica a pesar de que la foto solamente se subió una vez, pues dicha foto puede ser compartida y reenviada en innumerables ocasiones. En cambio, un mensaje de texto ofensivo sí puede considerarse agresión esporádica si no hace parte de un patrón de agresiones y es enviado solamente a la persona agredida (MEN, 2013a, pág. 49).

- ***Acoso escolar o bullying:*** "conducta negativa, intencional, metódica y sistemática de agresión, intimidación, humillación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza o incitación a la violencia o cualquier forma de maltrato psicológico, verbal, físico o por medios electrónicos contra un niña, niño o adolescente, por parte de un estudiante o varios de sus pares con quienes mantiene una relación de poder asimétrica, y que se presenta de forma reiterada o a lo largo de un tiempo de terminado".*

Tipología de eventos según ley 1620:

- ***Tipo I:*** corresponden a este tipo los conflictos manejados inadecuadamente y aquellas situaciones esporádicas que inciden negativamente en el clima escolar, y que en ningún caso generan daños al cuerpo o a la salud.

- ***Tipo II:*** corresponden a este tipo las situaciones de agresión escolar, acoso escolar (bullying) y ciberacoso (ciberbullying), que no revistan las características de la comisión de un delito y que cumplan con cualquiera de las siguientes características:

  a) Que se presenten de manera repetida o sistemática.
  b) Que causen daños al cuerpo o a la salud sin generar incapacidad alguna para cualquiera de los involucrados.

- ***Tipo III:*** corresponden a este tipo las situaciones de agresión escolar que sean constitutivas de presuntos delitos contra la libertad, integridad y formación sexual, referidos en el Título IV del Libro II de la Ley 599 de 2000, o cuando constituyen cualquier otro delito establecido en la Ley penal colombiana vigente

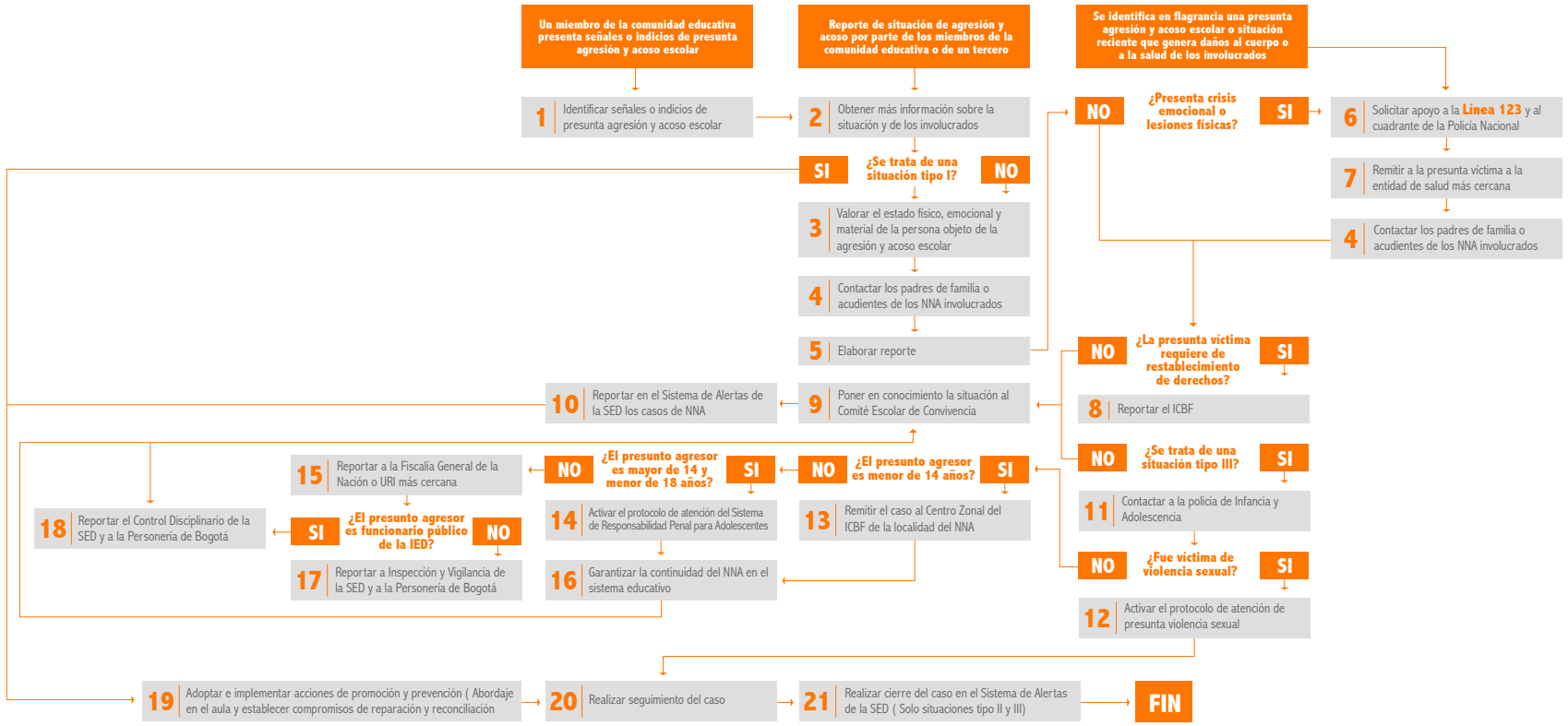
Señales o indicios de presunta agresión y acoso escolar de quien es víctima

- Hematomas o heridas en el cuerpo.
- Fuerza, tamaño y aspecto físico percibidos como inferiores.
- Pérdida de apetito o sueño.
- Estado permanente de alerta.
- Temor manifiesto.
- Vergüenza.
- Irritabilidad.
- Baja autoestima.
- Sentimiento de culpa.
- Depresión.
- Dificultad para hacer amigos o hablar en público.
- Rigidez.
- Aislamiento.
- Tendencia al bajo desempeño escolar y ausencias injustificadas.
- Desconfianza, miedo y ansiedad ante la socialización.
- Retraimiento social y desmotivación constante.

De quien ejerce la agresión y acoso:

- Conducta agresiva.
- Participación en actividades impropias de la edad (vandalismo, prostitución).
- Robo de comida, objetos y dinero.
- Conductas disruptivas consigo mismo, con niños más pequeños o con animales.
- Obligación de trabajo excesivo o asunción de roles de parentalización (cuidado de la casa, cuidado de hermanos).
- Consumo de SPA.
- Intimidar a través de la percepción de superioridad en fuerza y tamaño físico.
- No tolerar disensos respecto al punto de vista propio.
- Pretender someter y discriminar constantemente a otros.
- Relacionamientos exaltados, impulsivos y poco empáticos.
- Indisposición u oposición al acatamiento de regla.
- Tendencia y miedo constante a la frustración.
- Necesidad de ser vistas como personas poderosas y agresivas.

Diagrama de atención



Para saber más

Ministerio de las TIC
https://www.enticconfio.gov.co/

Ministerio de las TIC – YouTube
https://www.youtube.com/channel/UCow4aaqr3MuJP7u76rYlzNA

Policía Nacional
https://www.policia.gov.co/denuncia-virtual/delitos-informaticos

Teprotejo
https://teprotejo.org/

ICBF
https://www.icbf.gov.co/mis-manos-te-ensenan/que-hacer-si-eres-victima-o-te-enteras-de-un-caso-de-sexting

Secretaría de Educación del Distrito
Avenida El Dorado No. 66 -63
Teléfono (57+1) 324 10 00
Bogotá D.C. - Colombia

www.educacionbogota.edu.co

@Educacionbogota
Educacionbogota
/Educacionbogota
@educacion_bogota

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ