PROTOCOLO Y SUGERENCIAS FRENTE AL USO DE INTERNET, REDES SOCIALES y ELEMENTOS TECNOLÓGICOS

2024

PROTOCOLO Y SUGERENCIAS FRENTE AL USO DE INTERNET, REDES SOCIALES y ELEMENTOS TECNOLÓGICOS

- **Definiciones generales**

Ciberbullying

Resulta de la mayor urgencia que los estudiantes desarrollen habilidades para identificar, evitar y defenderse de los peligros y amenazas que se les puedan presentar cuando navegan por Internet y sobre el uso de las redes sociales.

También queremos regular en estos procedimientos el uso de celular.

Son múltiples los riesgos a los que se enfrenta la niñez, la juventud (y la sociedad en general) cuando acceden a Internet.

Se deben acometer con toda seriedad acciones tendientes a lograr que los menores adopten conductas responsables y preventivas, cuando navegan y se interrelacionan con otras personas en Internet.

Estas acciones tienen carácter de urgencia pues las Tecnologías de la Información y las Comunicaciones (TIC) llegaron para quedarse y hacer presencia en todos los ámbitos de la sociedad. Más urgentes aún, si tenemos en cuenta que la niñez y la juventud están cada día más expuestas a computadores y dispositivos móviles que ofrecen conexión a Internet.

Concretamente, son cada vez más los hogares que cuentan con acceso a Internet y, en el campo educativo, muchos Establecimientos educacionales actualmente implementan iniciativas transformadoras tales como integrar servicios Web 2.0 en los procesos educativos, un computador portátil por estudiante, etc; todo lo anterior, con Internet de por medio.

Ahora, si bien es cierto que estas iniciativas ofrecen beneficios inmensos para docentes y estudiantes, también conllevan potenciales riesgos y responsabilidades por parte del usuario. Por esto resulta de la mayor urgencia que los estudiantes desarrollen habilidades para identificar, evitar y defenderse de los peligros y amenazas que se les puedan presentar cuando navegan por Internet y cuando interactúan a través de redes sociales.

Afortunadamente, se viene registrando ahora un aumento significativo de propuestas que buscan concientizar a docentes, padres de familia y estudiantes sobre la importancia de respetar un código de conducta básico cuando se usa Internet.

Cuando se presenten situaciones que afectan a estudiantes del establecimiento, aunque sea a través de redes sociales, en horarios y lugares distintos al colegio, pero que afecten a algún miembro de nuestra comunidad escolar consideraremos los mismos elementos que hemos descrito en todos los protocolos, como son identificación de las conductas, responsables, plazos y acciones concretas que permitan abordar la situación.

❖ **Protocolo en caso de Ciberbullying:**

1. Uso de páginas prohibidas (por su contenido)
2. Uso de software prohibidos (por su contenido)
3. Uso de links prohibidos (por su contenido)
4. Uso de aplicaciones prohibidas (por su contenido)
5. Uso de imágenes con contenido sexual y/o personales.
6. Uso de claves y/o contraseñas de otros miembros de la comunidad (como compañeros y/u otros).

❖ **Procedimiento:**

1. Constatar la información, en lo posible con el link, la página, las imágenes, el contenido descrito, etc., con un print de pantalla o una impresión de lo observado en dicho medio. Apenas se reciba la información, lo realizará el encargado de convivencia escolar.
2. Acoger todas las denuncias que se presenten, ya sea verbal y/o presencialmente y/o por escrito. Siempre se mantendrá en convivencia escolar un formulario escrito donde se acogerán todas las denuncias de este tipo. El encargado de convivencia es el responsable de recibir las denuncias y él se encargará de delegar, esta tarea a parte del equipo de convivencia escolar.
3. Realizar una recopilación de antecedentes, con la información de todos los involucrados. Desde recibida la denuncia, y hasta un plazo máximo de tres días en esta primera etapa.
4. Levantar un acta con toda la información aportada por todos los intervinientes. Este documento se mantendrá en el equipo de convivencia escolar, y lo administrará dicho equipo.
5. Evaluar los antecedentes y si estos son suficientes, fundamentar la denuncia inicial. Transcurrida la primera etapa de tres días, el encargado de convivencia o quien el delegue, ponderará dicha información gestionará los pasos siguientes o bien dará una respuesta formal y por escrito al denunciante.
6. Entrevistarse con los padres de los involucrados. En la etapa de evaluación de antecedentes (desde el tercer día en adelante) se entrevistará a los padres, para conocer si tienen información relevante sobre la denuncia original y con el propósito de aportar en esta etapa de recopilación de antecedentes.
7. Aplicar sanciones y/o medidas disciplinarias en los casos que lo amerite. Al término de esta primera etapa, es decir, entre el tercero y décimo día, se concluirá y se dará cierre a la denuncia original con o sin sanciones, por parte del encargado de convivencia escolar.
8. Acoger a todos los involucrados con apoyo Psicosocial, para hacer contención y las derivaciones que correspondan, según el daño producido a él o los estudiantes involucrados. Luego del cierre y de la evacuación del informe, se pronunciará acerca de la necesidad de algún tipo de apoyo profesional, en caso de requerirlo, o bien se trabajará como equipo de convivencia con el estudiante.
9. Nunca dar por desestimada una denuncia, sin todos los antecedentes. Esto es fundamental para la protección de los derechos de los niños. En caso de que los agresores, sean estudiantes de otro establecimiento, el encargado de convivencia, informará a los apoderados de la estudiante, para que inicien acciones con el establecimiento, al cual asisten los otros estudiantes.
10. Se tomarán medidas de resguardo y /o protección, según se evalúe (el equipo de

convivencia escolar) con las estudiantes y los padres de las niñas, además de todos los involucrados, como son:

a) Cambio de curso

b) Evaluación por profesionales externos, dependiendo del tipo de situación, para que se realice un diagnóstico de la estudiante.

c) Monitoreo y seguimiento por parte de los profesionales del equipo de convivencia, al tratamiento que se aplicará a la estudiante.

d) Levantamiento de información relevante.

e) Evaluación de la condición del estudiante, transcurrido una semana, dos semanas, un mes, dependiendo del diagnóstico.

f) Evaluación del tratamiento aplicado a la estudiante y la derivación y/o cierre del caso, dependiendo a la evolución de la niña.

Es fundamental que se pondere como equipo de convivencia escolar, si las acciones aplicadas a la estudiante, son suficientes y sino hacer las coordinaciones necesarias con la familia de la estudiante, para resguardar la integridad de la niña.

- **Procedimientos en caso de utilización de equipos electrónicos, celulares, ipad, Tablet y/u otros.**

El colegio es un espacio de socialización y es verdad que los celulares no ayudan mucho en ese sentido. De igual forma si estos teléfonos no se usan con un fin pedagógico en clases, son un objeto de distracción que poco ayuda en el aprendizaje de nuestras niñas.

Sin embargo, esta realidad ha venido para quedarse. Las nuevas generaciones de jóvenes, también denominados 4G viven en un mundo los dispositivos digitales (celulares inteligentes, tabletas y videojuegos), son de un amplio y masivo acceso. Luchas contra eso no es lo más conveniente ni sensato, como lo señalan diversos estudios y las propias instituciones.

Prohibir solo por prohibir no es una buena medida, puesto que hay asignaturas donde un celular si puede ser una gran herramienta, y hay otras, claro, a las que su uso no aporta en nada. Según lo señala la Agencia de la calidad.

Es por esto que proponemos el siguiente procedimiento, para abordar esta problemática.

- **Dentro del aula y en clases:**

Si el estudiante trae al establecimiento, porta, mantiene en su poder algún tipo de dispositivo electrónico, como iPad, Tablet, celular, etc., lo hará bajo la absoluta responsabilidad de los padres y apoderados, por tanto, en caso de pérdida o extravío, el colegio no se hace responsable, ya que considerando el valor de estos equipos, el propósito de las actividades y el uso de estos implementos, el establecimiento, no lo tiene considerado en su planificación, ni en su trabajo diario. Por lo que se le solicita a los padres y apoderados, abstenerse de enviar a las niñas con estos implementos. Si a pesar de lo anterior la estudiante, trae algún equipo de los mencionados, con el objetivo de mantener comunicación con sus padres y/o apoderados, por motivos de coordinación y entrada y salida, al colegio, entrada y salida del establecimiento, se permitirá excepcionalmente en las siguientes condiciones:

1. Está Prohibido utilizar el o los equipo(s), durante las horas de clases.

2. Se sugiere que los equipos queden en un mismo lugar, dentro del aula y deben permanecer en silencio, durante todo el tiempo de clases.

3. Sólo se atenderán emergencias, cuando se justifiquen.

4. El celular y/o cualquier equipo se podrá utilizar sólo en los recreos.
5. Es importante señalar qué si la estudiante no obedece dicha instrucción, eventualmente se le aplicarán medidas disciplinas, si incurre y repite dicha falta.
6. Cuando la estudiante persista en desobedecer sistemáticamente a la instrucción señalada, es decir, siga utilizando el equipo en los tiempos señalados en que no lo debe hacer, Convivencia escolar, enviará una carta de amonestación al apoderado y se registrará dicha situación en el libro de clases.
7. Si a pesar de la amonestación anterior, la estudiante persiste en dicha conducta y siga utilizando el celular en la hora de clases, se citará al apoderado y se le prohibirá el uso de dicho implemento.
8. Para efecto de aplicar una medida pedagógica y/o formativa, se espera que el estudiante en su trayectoria pueda conversar con sus padres, y sus profesores, dicha actitud.
9. También se espera que la estudiante, tome conciencia del problema que genera su actitud al interior del aula, para ella misma, para el profesor, para el resto de sus compañeros y el resto de la comunidad escolar.
10. Se realizará taller de ciberbullying, redes sociales y uso de aparatos tecnológicos en el colegio, a las estudiantes de nuestra comunidad escolar.

- **Fuera del aula y fuera de clases:**

1. Está permitido utilizar dichos equipos al exterior del aula y fuera de los tiempos de clases.
2. Se espera que los padres y apoderados, supervisen el uso de equipos en los espacios fuera del colegio, como son: internet, redes sociales, páginas web, etc., para que la estudiante pueda comprender el daño que podría producir el uso indiscriminado de este tipo de implementos, considerando la etapa del desarrollo de la niña.

❖ RECOMENDACIONES PARA DOCENTES

A continuación, ofrecemos una serie de recomendaciones a tener en cuenta por parte de los docentes, cuando realizan actividades educativas enriquecidas con Internet y los procedimientos de actuación frente al uso de celulares, equipos informáticos, internet y las redes sociales:

- **Dentro del establecimiento:**

1. Informe a los estudiantes que el reglamento de uso de las salas de informática, de la red escolar y del acceso a Internet, prohíbe expresamente navegar por páginas con contenido inapropiado para menores; explique que no atender esta norma acarreará sanciones.
2. Comunique claramente a los estudiantes que está prohibido descargar cualquier software de Internet, sin la debida autorización y sin la presencia de un(a) docente.
3. Cuando sea necesario, permita que se descarguen aplicaciones únicamente desde sitios Web oficiales. Muchos sitios simulan ofrecer programas populares que se alteran, modifican o suplantan por versiones que contienen algún tipo de virus o software malintencionado (malware) y que infectan el computador cuando el usuario lo instala en el sistema. - Indique a sus estudiantes que eviten hacer clic en enlaces sospechosos. Los enlaces son uno de los medios más utilizados para direccionarlos a páginas Web que tienen amenazas capaces de infectar el

computador del usuario con virus o software malintencionado/espía.

4. Informe a los estudiantes sobre las responsabilidades civiles, penales o administrativas que existen cuando se vulneran derechos propios o de terceros en la red.
5. Asegúrese que los estudiantes son conscientes de que la distribución de contenidos prohibidos por la Ley (en especial la pornografía infantil), el acoso (en especial el acoso sexual), la discriminación, la promoción del odio racial, la difamación y la violencia, entre otros, son ilegales en Internet y en las redes sociales. Estas conductas se castigan con cárcel, según el código penal.
6. Evite que los estudiantes ingresen información personal en formularios Web de dudosa procedencia. Cuando un formulario contiene campos con información sensible (por ejemplo, usuario y contraseña), es recomendable verificar la legitimidad del sitio.
7. Notifique a los estudiantes que se requiere tanto la autorización como la presencia de un(a) docente en la sala de informática para que ellos puedan utilizar Chats, IRC, servicios en línea de comunicación en tiempo real y redes sociales.
8. Asegúrese que los estudiantes comprenden que no deben invadir la privacidad de otras personas cuando interactúan con ellas por medio de redes sociales.
9. Muchas de las "riñas virtuales" que se convierten en "cyberbullying", se inician porque una de las partes no observa buenas maneras al comunicarse por Internet. Explique a sus estudiantes las normas básicas de "Netiqueta" (La Netiqueta y sus 10 Reglas Básicas. En Internet convivimos muchos usuarios. ... Es un conjunto de reglas que regulan el comportamiento de los usuarios para comunicarse en la red, en pocas palabras es la etiqueta del ciberespacio), y asegúrese que las cumplen cuando se comunican con otras personas.
10. Esté atento al comportamiento de los estudiantes cuando utilicen redes sociales en Internet, con el fin de detectar y evitar situaciones de ciberacoso (responsable: menor/adulto; víctima: adulto), de "cyberbullying" (responsable: menor; víctima: menor) o de Grooming (responsable: adulto; víctima: menor).
11. Antes de que los estudiantes envíen a otras personas a través del correo electrónico, mensajería instantánea o redes sociales, promueva el hábito de reflexionar y evaluar la conveniencia de que esas personas conozcan dicha información y los riesgos que esto puede representar para su seguridad personal o familiar.
12. Asegúrese que los estudiantes entienden que, al participar en redes sociales, existe la posibilidad de encontrarse con personas que no son quienes dicen ser y que desean aprovecharse de otras personas.
13. Reflexione con los estudiantes sobre los aspectos positivos del uso de pseudónimos como medio de protección en las redes sociales, mensajería instantánea, chats y foros. Además, sobre el uso responsable de estos pseudónimos que, entre otras cosas, implica no utilizarlos para engañar o confundir a otros.
14. Tenga en cuenta que la legislación requiere autorización expresa de los padres o acudientes antes de permitir a menores de 14 años participar en actividades educativas en las que se utilice correo electrónico, blogs, wikis, servicios de mensajería instantánea, redes sociales, etc. También hay que Solicitar autorización cuando se utilizan servicios en línea que pueden almacenar alguna información sensible acerca de los estudiantes.
15. Diseñe y realice un taller para padres en el que se informe a estos los riesgos que. corren sus hijos cuando, sin control alguno, navegan en Internet o se comunican con

otras personas. Comparta y discuta con ellos la sección "Recomendaciones para padres", que encontrará más abajo en este mismo documento.

16. Destine un espacio en el currículo de las asignaturas para socializar con los estudiantes las "Recomendaciones para estudiantes" que encontrará más abajo en este documento.
17. Conozca y tenga a mano los números telefónicos y las páginas Web de la PDI y/o fiscalía, ante las cuales denunciar delitos informáticos.
18. Consulte con frecuencia sitios especializados en Internet Seguro para mantenerse al tanto de las últimas amenazas (spam, phishing, fraude electrónico, robo de identidad, etc) y de la forma de prevenirlas.

❖ RECOMENDACIONES PARA ESTUDIANTES

Cuando navego y cuando me relaciono con otras personas en Internet, pongo realmente todo mi empeño para no causar daño a nadie y para mantenerme alejado de amenazas y problemas. Por lo tanto, me comprometo a:

1. No dar nunca, a personas que no conozca de manera presencial, mi información personal (dirección particular, número de teléfono, etc.), mí Institución Educativa (nombre, ubicación, etc.) o mí familia (nombres de padres y hermanos, etc.).
2. Respetar la información que tengo de mis amigos y no publicarla en Internet sin su autorización explícita y por escrito.
3. No revelar nunca a nadie, que no sean mis padres o acudientes (ni siquiera a mis mejores amigos), mis claves de acceso al correo electrónico y a las redes sociales. Esto evitará que me suplanten.
4. Utilizar contraseñas fuertes, (o más seguras) difíciles de adivinar, con longitud de al menos 8 caracteres, que incluyan la combinación de números y letras.
5. Cerrar completamente tanto mis cuentas de correo electrónico como de redes sociales cuando termino de utilizar el computador.
6. No enviar nunca fotografías mías o de mis familiares, sin el permiso de mis padres.
7. Informar a padres y profesores cuando encuentre información que me haga sentir incómodo(a) y/o amenazado(a).
8. No realizar procedimientos en Internet que cuesten dinero, sin el permiso de mis padres.
9. 9. Nunca contestar a mensajes que sean agresivos, obscenos, amenazantes o que me hagan sentir mal o amenazado.
10. No responder correos electrónicos de personas que yo no conozca personalmente.
11. Avisar a padres y docentes cuando alguien me ofrezca un regalo y me suministre una dirección a la que deba ir para recibirlo.
12. No aceptar citas de desconocidos y avisar inmediatamente a padres y docentes. Considerar que hay personas que no siempre son lo que dicen ser.
13. Desconfiar de aquellas personas recién conocidas que quieren verme por medio de la cámara Web del computador o que encienden su cámara sin que yo lo haya solicitado.
14. Cuidarme en los ambientes tecnológicos como lo haría cuando salgo a la calle; utilizando mi criterio para seleccionar los sitios que visito en la Red y las personas con las que interactúo.
15. No permitirles a mis amigos por Internet, cosas que no les permito a mis amigos del colegio o del barrio.

16. Permitir, en las redes sociales en las que participo (Facebook, Hi5, MySpace, etc), que únicamente mis amigos puedan ver y comentar lo que comparto, lo que publico en el muro y en lo que yo esté etiquetado.
17. Permitir, en las redes sociales en las que participo (Facebook, Hi5, etc), que solamente mis amigos puedan ver mi información de contacto y mis fotografías.
18. Reflexionar, antes de subir una fotografía a un sitio social, si la foto se presta para que otra persona la descargue y me haga daño a mí o a otras personas.
19. Aceptar solicitudes de amistad en redes sociales que provengan únicamente de personas conocidas.
20. No utilizar, en las redes sociales en las que participo, identidades falsas para suplantar personas.
21. Nunca descargar, instalar o copiar nada de Internet sin el permiso previo de padres o docentes.

❖ RECOMENDACIONES PARA PADRES

Atender los siguientes consejos minimiza los riesgos que pueden correr sus hijos cuando utilizan Internet:

1. De a sus hijos buen ejemplo cuando navegue por Internet y cuando se relacione en redes sociales con otras personas.
2. Hable frecuente y abiertamente con sus hijos sobre posibles riesgos que existen en Internet.
3. Acompañe a sus hijos a navegar en Internet; conozca y evalúe cuáles son sus sitios favoritos y las redes sociales en las que participan.
4. No permita que sus hijos se conviertan en huérfanos digitales. Esto sucede cuando los padres de familia no acompañan a sus hijos en el uso de las TIC, creando una brecha con ellos al no comprender ni hablar el lenguaje digital imperante hoy en día.
5. Configure el "SafeSearch" (SafeSearch es un filtro del buscador Google que tiene por objetivo proteger a los niños de páginas web e imágenes que se consideran únicamente para adultos, como pornografía y otro contenido potencialmente ofensivo. Este filtro debe de ser habilitado para que entre en función y, es recomendable que lo actives en tu cuenta de Google)del motor de búsqueda de Google para evitar que aparezcan páginas con contenido sexual explícito entre los resultados de una búsqueda. Seleccione la opción "Utilizar el filtro estricto"; este filtra tanto texto explícito como imágenes explícitas. - Ubique el computador en áreas comunes del hogar (estudio, sala, etc). Para una delincuente resulta más difícil comunicarse con un menor cuando el computador está en un lugar a la vista de todos los que habitan el hogar.
6. Cuando sus hijos utilicen en casa un computador con cámara Web, adviértales que dicha cámara solo se debe usar en comunicaciones con personas conocidas.
7. Tenga en cuenta que cuando los menores son objeto de ciberacoso, "cyberbullying" o de Grooming, casi nunca lo manifiestan voluntariamente. Por lo regular guardan silencio sobre este problema, haciendo que esta práctica sea muy difícil de detectar y eliminar.
8. Muestre a sus hijos cómo respetar a los demás cuando se usa Internet y asegúrese de que comprendan que las reglas del buen comportamiento no cambian respecto a las presenciales, sólo porque estén frente a un computador.
9. Acompañe a sus hijos cuando asisten a un café Internet a realizar alguna consulta o tarea. Nunca se sabe quién se va a sentar al lado de ellos y la función de quien atiende el lugar

no es cuidar a los niños para que los demás clientes no se les acerquen.

10. Averigüe qué acciones ejecutan actualmente en la Institución Educativa donde estudian sus hijos para hacer que el acceso a Internet dentro de la Institución sea seguro. Ventile este tema abiertamente en las reuniones de padres de familia.
11. Elabore un reglamento con normas claras para el uso de Internet en el hogar (horario, duración de la conexión, forma de uso) y comuníquelo a sus hijos. Además, vigile su cumplimiento. Recomendamos consultar el "Contrato de código de conducta en línea" propuesto por Microsoft.
12. Solicite una copia del reglamento de uso de las salas de informática, de la red escolar y del acceso a Internet de la Institución donde estudian sus hijos e incluya varias de las normas contenidas en este, en el reglamento para usar Internet en el hogar. Esto permite que el reglamento del hogar esté acorde con el del colegio.
13. Asegúrese que la conexión a Internet de su hogar es segura, especialmente si es inalámbrica. Protéjala siempre con una contraseña fuerte; de lo contrario, cualquier vecino se puede conectar a través de ella, restándole velocidad de navegación.
14. Si instala un router inalámbrico para tener acceso a Internet en el hogar, ubíquelo en un sitio al cual tengan acceso en todo momento personas adultas. De esta forma es más fácil controlar los horarios de acceso a la red ya que con solo desconectar el aparato de la fuente de energía, cesa el acceso a Internet.
15. Además de un antivirus, instale un firewall (cortafuego) en su computador. Este último impedirá que entre cualquier software malintencionado o que algún software espía que haya infectado el computador envíe datos sin que usted se dé cuenta.
16. Si sus hijos visitan salas de chat, utilizan programas de mensajería instantánea (como Messenger), videojuegos en línea u otras actividades en Internet que requieran un nombre de usuario para identificarse, ayúdeles a elegirlo y asegúrese de que dicho nombre no revela ninguna información personal.
17. Manténgase informado tanto de las últimas amenazas como de las herramientas informáticas para contrarrestarlas.
18. Enseñe a sus hijos, desde pequeños, a usar las TIC con responsabilidad.
19. Aleccione a sus hijos para que confíen en su propio instinto. Si algo en Internet los pone nerviosos, deben tener la suficiente confianza para expresarlo a un adulto responsable sin temor a que se les prohíba su uso o se les castigue.
20. Si su hijo, hija o joven ya participó en alguna actividad de tipo sexual por medio de Internet, comprenda que él o ella no son delincuentes, son víctimas. El delincuente que los sedujo es quien tiene toda la responsabilidad.
21. Conozca y tenga a mano los números telefónicos y las páginas Web de la PDI y/o Fiscalía, ante las cuales puede denunciar delitos informáticos.