PROTOCOLO FRENTE A VULNERACIÓN, AGRESIONES U HOSTIGAMIENTO POR REDES SOCIALES (CIBER-BULLYING Y/O CIBER-ACOSO) Y MAL USO DE DATOS CONFIDENCIALES POR CUALQUIER AGENTE DE LA COMUNIDAD EDUCATIVA.

Marco Regulatorio.

La ley 20.536 al pronunciarse sobre el acoso escolar plantea que éste no sólo se da en el establecimiento educacional de forma presencial sino que continua a través del ciber-acoso o ciber bullying, el cual se manifiesta con conductas de acoso a través de medios electrónicos y de comunicación como el correo electrónico, las redes sociales, blogs, mensajes de móvil, etc. …*" la agresión u hostigamiento reiterado, ya sea por medios tecnológicos o cualquier otro medio, tomando en cuenta su edad y condición". (Ley 20. 536, artículo 16 B, Mineduc (2011).*

Po otro lado como organización o empresa (establecimiento educacional) existe el deber de protección de datos personales como derecho fundamental conforme a La Ley de protección de datos en Chile, ley Nº 19.628.

Conceptualización.

¿Qué es el Ciber-bullying o ciber acoso?

El Cyberbullying es el acoso psicológico entre pares, a través de medios tecnológicos, puede manifestarse a través de amenazas, burlas, envío de mensajes ofensivos, provocación con vocabulario grosero, trato irrespetuoso, difamación, propagación de información personal entre otras cosas.

El Cyberbullying se caracteriza por:

-Ser situaciones sostenidas en el tiempo, excluyendo situaciones puntuales.
-Constituyen situaciones de hostigamiento psicológico, no necesariamente con contenido sexual, aunque puede existir en algunas situaciones.
-Se desarrolla a través de medios digitales (redes sociales u otras plataformas).
-El acosador puede ampararse bajo el anonimato o utilizar otras cuentas.
-Normalmente existen testigos que tienden a estar al tanto de la situación, pero no siempre actúan para denunciar o ayudar a la víctima a solucionar el problema.

El Cyberbullying puede producirse de distintas formas:

a) Acosos: envío constante y repetido de mensajes crueles o amenazas.
b) Denigración: crear o utilizar sitios webs, portales de internet u otras plataformas tecnológicas o virtuales con el objetivo deliberado de insultar o denostar a otras personas.
c) Injurias o calumnias: injurias es toda expresión articulada o ejecutada en deshonra, descredito o menosprecio de otra persona. La calumnia es la imputación de un delito determinado, pero falso, el propósito de estas acciones es denigrar, dañar la reputación de la otra persona, como también su honra.
d) Suplantación: Reemplaza la identidad de la víctima, creando un perfil falso en redes sociales u otros servicios web.
e) Usurpación de identidad: quitar la clave de internet de algún medio en redes sociales para utilizarla enviando material poco adecuado, embarazoso para otros y para la víctima.
f) Exclusión: intencionalmente excluir a alguien de un grupo en línea.
g) Peleas en línea: generar peleas a través de mensajes electrónicos con lenguaje vulgar, grosero y denigrante.
h) Amenazas: acto de provocar temor al otro expresándole una intención de daño a otro o a su familia, puede ser su honra, personal o propiedad.
i) Happy-slapping: acción de grabar, filmar o registrar agresiones y/o actos de violencia física, a través de celulares, cámaras u otros medios tecnológicos difundiendo las agresiones.
j) Grooming: acción premeditada de un adulto de acosar sexualmente a un niño mediante el uso de internet. El grooming solo lo ejercen los adultos hacia los menores y es un delito (Cabe dentro de Protocolo de agresiones sexuales o hechos de connotación sexual).

¿Qué es la Ley de protección de datos en Chile?

La Ley de protección de datos en Chile se rige actualmente por una única ley, la ley Nº 19.628, la cual fue publicada en 1999. En estos más de 20 años la realidad ha cambiado de forma radical y por eso el gobierno ya tiene en marcha un proyecto para actualizar esta ley y ajustarse a las normas internacionales y promovidas por la OCDE.

En el año 2018, con la modificación del artículo 19 Nº4 de la constitución, se estableció la

protección de datos personales como derecho fundamental. Esto permite que cualquier persona tiene derecho a la protección de sus datos personales y que el tratamiento y protección de sus datos se efectuará en la forma y condiciones que determine la ley.

Según estas leyes, se considera datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Desde el RUT, nombre y apellidos hasta dirección de correo electrónico, teléfono, lugar de residencia, edad, etc.

La ley de protección de datos en Chile tiene como objetivo principal garantizar el derecho a la privacidad y proteger los datos personales de las personas físicas. La Ley se aplica al tratamiento de datos personales realizado por todos los contribuyentes, particulares, empresas y organizaciones.

Bajo la Ley 19.628 sobre la protección de la vida privada, la cual resguarda la confidencialidad de los datos, menciona en su artículo 4 que: "el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.
La autorización debe constar por escrito. La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos".

De igual forma el Artículo 11 menciona que: "el responsable de los registros o bases donde

se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

En lo específico, por datos confidenciales, para nosotros como comunidad educativa entendemos: números telefónicos, fotografías personales, informes confidenciales, diagnósticos clínicos de funcionarios y estudiantes.

Por tanto, el Instituto Santa María, se compromete y busca proteger la confidencialidad de datos de todos los agentes de la comunidad educativa.

- Aplicabilidad.

El presente protocolo tendrá por referencia lo expuesto a fin de dar respuesta educativa frente la ocurrencia de situaciones o contenidos que comprometen la intimidad personal o la dignidad de quienes aparecen en ellos. Cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

- Aspectos Claves en Prevención y Abordaje del Ciber-acoso.

¿Qué puedo hacer si soy víctima de bullying en las redes sociales?

- ✓ Cambia las configuraciones de privacidad.
- ✓ Bloquea y elimina contactos.
- ✓ Mantén tus detalles personales en privado.
- ✓ Deja de lado tu teléfono o computadora por un tiempo.
- ✓ Guarda emails, textos, mensajes de acoso, capturas de pantalla y todo tipo de evidencias.
- ✓ Reporta el bullying en el momento que sucede.
- ✓ Cuéntale a un adulto en quien confíes.
- ✓ No respondas ningún mensaje intimidatorio o hiriente. No caigas en "el juego".
- ✓ Reporta cualquier amenaza grave al establecimiento o la Policía.

¿Cómo prevenir el Bullying en línea (ciberbullying o ciber acoso)?

- ✓ No contribuyas al bullying en línea, aun si tus amigos/as te incentivan a hacerlo.
- ✓ No incites a los que hacen bullying dándoles "me gusta" o compartiendo sus comentarios o posteos.
- ✓ No distribuyas rumores en línea. Alza tu voz contra los rumores y mala información.
- ✓ No reenvíes mensajes negativos.
- ✓ Defiende a otras personas que son víctimas de bullying en línea.
- ✓ Bloquea y reporta a quienes lo hacen
- ✓ Edúcate en ciudadanía y convivencia digital.

Intervención y Procedimiento.

Etapa	Descripción	Responsable	Tiempo
1. Recepción de la denuncia o Detección	Comunicación del ciberbullying, ciber acoso o mal uso de datos personales. Cualquier integrante de la comunidad educativa que tome conocimiento de estos hechos o situaciones DEBE informar a encargado de convivencia escolar y/o coordinación de ciclo.	-Encargado/a de Convivencia (E.C) -Coordinador/a de ciclo (C.C)	Dentro de las 24 horas de tomado conocimiento.
2. Acciones iniciales de abordaje	Entrevista de potencial afectado y recolección de evidencias.	E. de convivencia o miembro de la dupla psicosocial.	Entre 24 a 48 hora de la toma de conocimiento
	Aviso a Dirección. Reunión inicial para valorar la situación con la coord. Ciclo Se define pertinencia o no de denuncia inmediata.	E.C o C.C	
	Aviso a la familia mediante entrevista	E.C o C.C	
	Aviso a Profesor jefe	E.C o C.C	

3. Adopción de medidas	Se podrá implementar si la situación lo amerita medidas de resguardo con el objeto de proteger a la víctima, separándola del agresor. Ej. suspensión temporal de asistencia a clases del presunto agresor mientras dure la investigación invocando Ley Aula Segura.	Encargado/a de Convivencia (E.C) -Coordinador/a de ciclo (C.C)	Máximo 10 días de suspensión notificados por escrito.
4. Indagatoria o investigación interna	Entrevistas a todas las personas involucradas, tales como: estudiante/s y los apoderados del o los estudiantes (acosado y presunto acosador).	E.C y/o C.C	Para faltas gravísimas hasta 15 días de tiempo para la indagatoria e informe de cierre según RICE.
	Entrevista a Docente jefe y testigos Claves	E.C y/o C.C	
	Análisis de caso equipo de gestión de convivencia escolar (gestión de ciclo y/o de Pastoral, Formación y Convivencia.	Equipo de Conv. Escolar	
5. Resultados de Investigación Interna	Entrega de resultados a Dirección	E.C y/o C.C	A más tardar el día 10 de tomado conocimiento de la situación.
	Entrega de resultado a familias correspondientes		
	Entrega de resultado al prof. jefe		
6. Elaboración de informe de cierre de caso y resolución	Si la indagación demuestra que era verídica la denuncia, se aplicaran todas las medidas pedagógicas, formativas y de reparación del daño causado. Con las medidas sancionatorias y disciplinarias correspondientes. Se cita a ambas partes por separado y se le da a conocer el resultado.	E.C y/o C.C	A más tardar el día 10 de tomado conocimiento de la situación.
7. Apelación	En caso de que algunas de las partes no esté de acuerdo con la resolución podrá apelar por escrito a Dirección del establecimiento.	Familias a Dirección mediante carta escrita.	Plazo 48 horas posterior a la entrega de la resolución del colegio

8. Plan de Trabajo	El equipo de Convivencia Escolar, efectúa un plan de trabajo: realiza apoyo psicosocial y deriva de ser necesario a alguna red de apoyo al o los implicados. Acoge a la posible víctima, así como socio educa al posible agresor. Realizar intervención en clases de orientación a cargo del Profesor jefe en acompañamiento del Equipo de Convivencia, con el fin de enseñar sobre los nocivos efectos del ciberacoso, y reforzar la importancia del correcto uso de internet y las redes sociales en general	Profesionales del Equipo de Pastoral, Formación y Convivencia	Dentro del primer mes de los hechos y durante el semestre lectivo.
8. Monitoreo y seguimiento.	Monitoreo de estudiantes y revisión del factor relacional y de convivencia escolar.	Encargado de Conv. Escolar Coord. Ciclo Profesor jefe.	Durante el semestre académico o año lectivo