



## Política de Seguridad en línea

### A. Propósito

La Institución Educativa espera que todos los colaboradores en nuestro colegio desarrollen la capacidad de reconocer las acciones a seguir para promover el cuidado en línea de los estudiantes.

Ratificamos la importancia que radica sobre la protección de nuestros estudiantes, por lo cual toda la comunidad educativa debe ser capaz de identificar situaciones de riesgo y solicitar ayuda cuando sea necesario.

Si conoce los comportamientos y límites establecidos en esta política, se convertirá en un exitoso usuario electrónico en la Institución. Todo el uso electrónico en todas las escuelas de ISP, incluyendo las cosas que usted hace en el día a día, se regirá por este documento de política. Su uso correcto e incorrecto cualquier electrónica mientras que en la escuela será interpretado según esta política.

#### 1. Alcances y Objetivos

El Liceo Panamericano Centenario tiene como objetivo:

- Proveer un ambiente seguro y feliz que favorezca el desarrollo integral de nuestros estudiantes.
  - Definir un sistema de procedimientos que permita evaluar si los estudiantes están seguros en el ambiente escolar.
  - Generar conciencia en toda la comunidad educativa sobre la importancia del uso y/o cuidado en línea de los estudiantes.
  - Sostener una comunicación efectiva en toda la comunidad educativa respecto a temas relacionados a la seguridad en línea.
  - Establecer procedimientos claros y efectivos para los colaboradores que deban asumir alguna función relacionada a la seguridad en línea.
  - Socializar oportunamente con toda la comunidad educativa acerca de la Política de Seguridad en línea.
- **Estudiante:** se considera como estudiante a cualquier niño, niña y/o adolescente del Liceo Panamericano Centenario, sin importar su edad, así como visitantes que sean menores de edad.
- **Colaborador:** Todo miembro contratado por el Liceo Panamericano Centenario, sin importar su puesto o cargo.

### A. Alcance

La política de redes sociales será avalada y firmada por Rectorado. Esta política será adoptada por todos los niveles de la organización.

### B. Definiciones

El uso de las TIC en la educación puede ayudar a los estudiantes a desarrollar las competencias digitales y tecnológicas necesarias para llevar a cabo diferentes proyectos educativos.

La presente política tiene como objetivos identificar, caracterizar y prevenir el riesgo que las TIC conllevan en su uso, definiéndolo en grupos de riesgo: cyberbullying, grooming, sexting, malware, uso abusivo, vulneración de la propiedad intelectual y acceso a contenidos inapropiados.

### C. Responsabilidades

El Liceo Panamericano Centenario ofrece acceso a Internet, incluyendo el acceso al correo



electrónico institucional para estudiantes y colaboradores. Todo el acceso a Internet, incluyendo el uso del correo electrónico, se produce a través del uso del sistema del colegio.

Esta política de Seguridad en Línea rige toda la actividad electrónica, incluyendo el correo electrónico y el acceso a Internet, que es emprendido por estudiantes, colaboradores y padres y/o madres de familia, como parte de la educación, programas educacionales o extracurriculares conectados a la Institución. Ningún miembro de la comunidad educativa puede participar en actividades prohibidas por esta política, ya sea a través del servicio de Internet o a través de cualquier otro Proveedor de servicios de Internet, por cualquier razón. Se recomienda encarecidamente a los padres y/o madres que conversen y supervisen el uso de Internet en la escuela de su hijo/hija y de cualquier preocupación que puedan tener con docente y rectorado. Toda utilización de Internet se registrará por esta política.

- Salvaguardar los derechos del menor.
- Promover el bienestar del estudiante a través de prácticas que aseguren el respeto por su privacidad.
- Establecer procedimientos claros que brinden protección a los adultos que deben atender las necesidades de la seguridad en línea.
- Socializar con los padres de familia sobre los procedimientos aplicados sobre la seguridad en línea.
- Comunicar al Líder Designado de Salvaguarda cualquier inquietud sobre las prácticas de seguridad en línea.

#### ➤ FILTERING

El Liceo Panamericano Centenario ha instalado el software de filtrado de Internet en un intento de bloquear el acceso de los usuarios a contenidos inadecuados y/o dañinos en Internet. La tecnología de filtrado no es perfecta y, por lo tanto, puede interferir con la investigación educativa legítima. Ningún software de filtrado es 100 por ciento efectivo y ocasionalmente falla. El filtro se establece en la configuración más restrictiva en restringir el acceso a sitios de Internet que pueden contener chat o correo interactivo o información sobre:

- Actos sexuales
- vestimenta sexual
- sexo/desnudez
- sexo/personal
- deportes
- de juego
- pornografía
- hacking
- de la evitación del proxy
- adicciones
- foros
- redes sociales
- Violencia
- streaming Music
- videos no académicos
- drogas ilegales
- armas
- actividad delictiva
- chat
- odio e intolerancia

#### D.Regulaciones de Access

- Consecuencias importantes del acceso
  - a) Liceo Panamericano Centenario siempre cooperará plenamente con funcionarios locales, y/o estatales en cualquier investigación legal concerniente o relacionada con cualquier actividad ilegal conducida a través del uso del internet.
  - b) El acceso a Internet es un privilegio, no un derecho, y todos los estudiantes deben ser conscientes de que el Liceo Panamericano Centenario puede revocar el acceso



a Internet por cualquier razón. Si el acceso de un estudiante es revocado, proporcionará una explicación para la revocación, y se asegurará de que el estudiante continúe teniendo igual acceso para participar en el programa educacional.

- c) Es muy importante que los estudiantes y las familias comprendan que las violaciones de este Internet y la política de Seguridad en línea cuentan con acciones disciplinarias. Todas las infracciones de esta política serán atendidas de acuerdo con el plan disciplinario de la Institución. Los estudiantes y sus familias tendrán que cumplir con preocupaciones específicas relacionadas con la violación y cooperar con la Institución para ayudar al estudiante a adquirir los comportamientos específicos necesarios para comportarse apropiadamente.

- Privacidad

Es importante que todos los colaboradores y estudiantes entiendan que no hay expectativa de privacidad en este sistema

- a) El Liceo Panamericano Centenario se reserva el derecho de monitorear el uso de Internet a través de su Dpto. de Sistema en todo momento. Se recopilará y almacenará información sobre el uso que incluye, pero no puede limitarse a la fecha y hora en que un estudiante visita el sitio e información sobre las actividades del usuario mientras está en línea. Cualquier información recopilada se obtiene únicamente con el propósito de mejorar los servicios de la Institución y proporcionar al sistema información estadística para ayudar a mejorar la enseñanza y el aprendizaje de los profesores y estudiantes, respectivamente. Salvo que se disponga lo contrario en esta política, Liceo Panamericano Centenario no utilizará cookies para recopilar información de identificación personal acerca de cualquier usuario.
- b) Según lo requerido por la LOEI, Liceo Panamericano Centenario monitoreará las actividades en línea de los estudiantes. Este monitoreo puede llevar al descubrimiento de que el usuario ha violado o puede estar violando, la política. Asimismo, se reserva el derecho de monitorear a otros usuarios (por ejemplo, no estudiantes) actividades en línea.
- c) Se reserva el derecho de emplear y revisar los resultados del software que busca, monitorea y/o identificarlas posibles violaciones de Internet y la política de uso aceptable de los dispositivos de la Institución.
- d) Los estudiantes deben ser conscientes de que sus archivos personales pueden ser descubiertos en procedimientos judiciales y administrativos y de acuerdo con las leyes.
- e) Los estudiantes no deben tener ninguna expectativa de privacidad en el contenido de sus archivos personales y registros de su actividad en línea mientras estén en la Institución. Liceo Panamericano Centenario no alienta a los estudiantes a almacenar datos personales en los dispositivos de la Institución y no puede ser responsable de la pérdida o daño de dichos datos.

## E. Notificación y responsabilidad parental

El uso del control parental es muy indexado por la seguridad en todos los ambientes, pero, sobre todo, en los ambientes educativos.

Realmente, desde el momento en sí que se aplica control y más orientado a nuestro niños, niñas y adolescentes, estamos haciendo prevención y por supuesto que se tiene que aplicar en la navegación de internet dentro y fuera de la Institución, no tan solo en laboratorios, en toda la navegación en su conjunto, inclusive Wifi abierto.

1. El Liceo Panamericano Centenario proporcionará a los estudiantes y a los padres



- pautas e instrucciones para la seguridad del estudiante mientras usan el Internet
2. La política de Seguridad en línea y dispositivos del Liceo Panamericano Centenario contiene restricciones al acceso a material inadecuado. Sin embargo, hay una amplia gama de materiales disponibles en Internet, algunos de los cuales pueden o no ajustarse a los valores particulares de los estudiantes. Mientras que el uso del estudiante será supervisado y registrado, no es prácticamente posible que el Liceo Panamericano Centenario supervise y haga cumplir una amplia gama de valores sociales en el uso de Internet por los estudiantes. Además, se reconoce que los padres tienen la responsabilidad primordial de transmitir su conjunto particular de valores familiares a sus hijos.

El Liceo Panamericano Centenario recomienda encarecidamente a los padres y/o madres de familia que especifiquen a sus hijos/hijas qué material es y no es aceptable para que sus hijos tengan acceso a través de las redes de la Institución.

## **F. Acceso**

Los estudiantes y colaboradores generalmente serán proveídos con acceso a Internet. Este documento describe los términos de ese acceso.

## **G. Limitaciones en el uso de Internet**

### **a) *Violaciones de seguridad personal para estudiantes:***

Liceo Panamericano Centenario recomienda encarecidamente que todos los estudiantes sigan las dos pautas a continuación, en todo momento:

- Los estudiantes no publiquen ni transmitan fotografías o información de contacto personal sobre ellos mismos o sobre otras personas.
- No subir fotos y/o videos con el uniforme del colegio ni que proporcionen ubicación de la Institución.
- Los estudiantes no deben aceptar reunirse con alguien que hayan conocido en línea.

Cualquier mensaje electrónico que reciban que sea inapropiado o los haga sentir incómodos, los estudiantes y/o colaboradores deben comunicar a la Líder de Salvaguarda.

### **b) *Actividades ilegales:***

Todos los estudiantes deben saber que participar en cualquiera de las siguientes actividades ilegales resultará en una acción disciplinaria por parte de la Institución.

Las actividades son:

- Intentar obtener acceso no autorizado al sistema de la Institución ni a ningún otro sistema informático ni ir más allá de su acceso autorizado. Esta prohibición incluye la búsqueda intencional de información sobre contraseñas pertenecientes a otros estudiantes, la modificación de contraseñas pertenecientes, la obtención ilegal de claves de acceso inalámbricas o el intento de iniciar sesión a través de la cuenta de otra persona. Además, los estudiantes no pueden intentar acceder, copiar o modificar los archivos de otro. Estas acciones no están permitidas y pueden ser ilegales, aunque solo sea con el propósito de "navegar".
- Intentar subvertir la seguridad de la red, es un proceso disciplinario que puede perjudicar la funcionalidad de la red o eludir las restricciones establecidas por los administradores de la red. También tienen prohibido destruir datos al propagar virus informáticos o dañar datos, software o equipos.
- No deberán usar el internet de la institución para participar en ningún otro acto ilegal, como organizar una venta de drogas, participar en actividades criminales de pandillas, amenazar la seguridad de una persona, etc. Asimismo, para descargar música ilegal, libros, videos y software sin pago al originador.



- Está prohibido usar aplicaciones de software que tengan una conexión continua a Internet que esté transmitiendo constantemente y consumiendo una gran cantidad de ancho de banda de Internet (por ejemplo, bit-torrent, etc.) con el fin de obtener contenido ilegal.

## H. Violaciones de seguridad del sistema

- a. Los estudiantes son responsables del uso de sus cuentas personales (correo electrónico, fb, IG, Tik-Tok, entre otros), si corresponde, y deben tomar todas las precauciones razonables para evitar que otros puedan usar su cuenta. Bajo ninguna circunstancia debe, un estudiante, proporcionar su contraseña a otra persona, excepto que el padre y/o madre de familia puede requerir que proporcione sus contraseñas.
- b. Los estudiantes notificarán inmediatamente a un colaborador si identifican un posible problema de seguridad (como la divulgación de su contraseña a otra persona) y el colaborador lo notificará inmediatamente al Líder de Salvaguarda. Ningún usuario buscará problemas de seguridad porque esto puede interpretarse como un intento legal de obtener acceso.

El Dpto. de Sistemas instalará y mantendrá el software antivirus en cada dispositivo de la Institución, según sea necesario. Las actualizaciones, generalmente denominadas "definiciones de virus", se actualizarán según recomiende dicho Dpto.

## I. Lenguaje inapropiado

Todos los estudiantes deben saber que el uso de un lenguaje inapropiado en forma electrónica puede dañar a otros y puede llevar a una acción disciplinaria. Esto son:

- Las restricciones contra el lenguaje inapropiado se aplican a mensajes públicos, mensajes privados y material publicado en páginas web.
- Los estudiantes no utilizarán lenguaje obsceno, profano, lascivo, vulgar, grosero, inflamatorio, amenazante, abusivo o irrespetuoso.
- No publicarán información que pueda interferir con el proceso educativo o causar un peligro de interrupción en el entorno educativo.
- No participarán en ataques personales, incluidos ataques perjudiciales o discriminatorios.
- No se podrá subir fotos y/o videos con el uniforme de la Institución a las redes sociales.
- Los estudiantes no acosarán a otra persona. El acoso persiste actuando de una manera que angustia o molesta a otra persona. Si un estudiante le dice a otro que deje de enviarles mensajes, debe detenerse.
- Los estudiantes no enviarán intencional o imprudentemente información falsa o difamatoria sobre una persona u organización.
- Los estudiantes no deben volver a publicar un mensaje que se les envió de forma privada sin el permiso de la persona que les envió el mensaje.
- Los estudiantes no deben publicar información privada sobre otra persona.

## J. Respetar los límites de recursos

- I. Los estudiantes y colaboradores utilizarán la red de la Institución solo para actividades



educativas y profesionales.

- II. Los estudiantes y colaboradores no descargarán archivos grandes a menos que sea absolutamente necesario. Si es necesario, los usuarios descargarán el archivo cuando el sistema no se esté utilizando en gran medida.
- III. Los estudiantes y colaboradores no publicarán cadenas de mensajes o participarán en "spamming". Enviar correos no deseados es enviar un mensaje molesto o no solicitado a muchas personas, excepto que un mensaje no solicitado enviado por un coordinador, jefe de Dpto. y/o rectorado, sea relacionado con la actividad laboral no constituye spam.
- IV. Los usuarios verificarán su correo electrónico con frecuencia y eliminarán los mensajes no deseados.
- V. Los usuarios no enviarán correos electrónicos que contengan enlaces comerciales a menos que el enlace sea predominantemente instructivo por naturaleza.

### **K. Plagio y violación de derechos de autor**

- Los estudiantes no plagiarán los trabajos que encuentren en Internet. Plagio es tomar las ideas o escritos de otros y presentarlos como si fueran originales para el usuario y su consecuencia es un proceso disciplinario.
- Los estudiantes respetarán los derechos de los propietarios de los derechos de autor y no infringirán esos derechos. La infracción de los derechos de autor ocurre cuando un individuo reproduce inapropiadamente un trabajo que está protegido por un derecho de autor. Si un trabajo contiene lenguaje que especifica el uso aceptable de ese trabajo, el usuario debe seguir los requisitos de las normas APA.

### **M. Acceso a material inapropiado**

- I. Los estudiantes no usarán el Internet de la Institución para acceder a material que sea profano u obsceno (por ejemplo, pornografía), que defienda actos ilegales o peligrosos, o que defienda la violencia o la discriminación hacia otras personas (por ejemplo, literatura de odio). Para los estudiantes, se puede hacer una excepción especial si el propósito es llevar a cabo una investigación y es aprobado por el docente y Coordinación Académica.
  - II. Si los estudiantes acceden inadvertidamente a dicha información, deben trascender de inmediato el acceso inadvertido a la Líder de Salvaguarda. Esto protegerá a los estudiantes contra una alegación de que han violado intencionalmente la política de Seguridad en Línea.
- ✓ Otro
- I. Los estudiantes no utilizarán Internet para publicidad, promoción, fines comerciales u objetivos similares.
  - II. Los estudiantes no usarán Internet para llevar a cabo actividades comerciales con fines de lucro.

### **N. Política de correo electrónico**

Los recursos de correo electrónico están disponibles para todos los estudiantes y colaboradores. Cada individuo asignado a una dirección de correo electrónico del Liceo Panamericano Centenario tendrá la responsabilidad de utilizar este recurso de manera eficiente, efectiva, ética y legal. Las siguientes acciones están prohibidas:



- ✓ Las actividades de correo electrónico "aceptables" son aquellas que se ajustan al propósito, los objetivos y la misión del Liceo Panamericano Centenario y a los deberes y responsabilidades del trabajo de cada colaborador. Los usuarios no tendrán derecho a la privacidad mientras usen el sistema de correo electrónico institucional.
- ✓ El uso "inaceptable" se define generalmente como actividades que utilizan hardware, software o redes del Liceo Panamericano Centenario en cualquier momento que no se ajusta al propósito, los objetivos y la misión de la institución y a los deberes y responsabilidades laborales de cada colaborador y estudiante. La siguiente lista, aunque no incluye, proporciona algunos ejemplos de usos inaceptables:
  - Apertura de archivos adjuntos de correo electrónico desconocidos o introducción de gusanos informáticos o virus. Los usuarios tienen prohibido realizar cualquier actividad que pueda causar la pérdida o corrupción de datos o el uso anormal de recursos informáticos (degradación del rendimiento del sistema / red).
  - El uso de servicios de correo electrónico para transacciones comerciales o comerciales privadas y cualquier actividad destinada a fomentar el beneficio personal.
  - Llevar a cabo actividades de recaudación de fondos o de relaciones públicas que no sean del Liceo Panamericano Centenario, tales como solicitar causas religiosas y políticas o actividades sin fines de lucro.
  - Transmitir información ofensiva amenazante y ofensiva (mensajes o imágenes) que contenga material difamatorio, abusivo, obsceno, pornográfico, de orientación sexual, racialmente ofensivo o tendencioso, discriminatorio o ilegal.
  - Intentar subvertir la seguridad de la red, perjudicar la funcionalidad de la red o eludir las restricciones establecidas por los administradores de la red. Ayudar a otros a violar estas reglas compartiendo información o contraseñas.
  - Distribuir correo "basura", como cadenas de cartas, anuncios o solicitudes no autorizadas.

**RECORDATORIO:** el Liceo Panamericano Centenario se reserva el derecho de examinar cualquier correo electrónico o correspondencia de Internet para fines de seguridad y / o administración de la red. La violación de esta política de correo electrónico puede resultar en una acción disciplinaria.

## O. Uso del dispositivo

Los dispositivos del Liceo Panamericano Centenario están disponibles para estudiantes y colaboradores autorizados con fines educativos, de investigación y administrativos. Para mantener esta política, es esencial que los usuarios observen estándares razonables de comportamiento con respecto al uso de los dispositivos.

Las siguientes acciones están prohibidas:

- Cualquier intento de modificar o dañar el equipo del dispositivo, incluyendo marcar el dispositivo de cualquier manera, colocar pegatinas o escribir en el dispositivo.
- Cualquier intento de modificar o dañar el dispositivo, la red o el software
- Cualquier intento de modificar las configuraciones originales del sistema
- Uso inapropiado del equipo del dispositivo
- Instalación de juegos no académicos
- Uso no autorizado de una cuenta que pertenece a otro usuario
- Lectura, uso o eliminación no autorizada de archivos privados o correos electrónicos pertenecientes a otro usuario
- Compartir nombre de usuario y contraseñas con otros usuarios o cualquier otra persona
- Cualquier intento de eludir (hackear / eludir) las funciones de seguridad y protección



- del sistema
- Usar conscientemente cualquier sistema para producir fallas del sistema o degradar el rendimiento
- Participar en la duplicación no autorizada, alteración o destrucción de datos, programas o software
- Transmitir o divulgar datos, programas o software que pertenecen a otros o duplicar materiales protegidos por derechos de autor.
- Uso de los recursos del dispositivo para fines privados, incluido, entre otros, el uso de los recursos del dispositivo con fines lucrativos o ilegales.

Liceo Panamericano Centenario se reserva el derecho de investigar cualquiera de los abusos anteriores, así como cualquier otra interferencia con el funcionamiento adecuado de la red o infracciones a los derechos de otro usuario. Cualquier violación dará como resultado una acción disciplinaria. Las consecuencias pueden incluir exigir a los estudiantes que respalden las reparaciones y el mantenimiento técnico (en consonancia con los principios de la justicia reparadora) o la pérdida del uso del dispositivo durante un período corto o prolongado. Si el abuso de los dispositivos es grave, puede incluir por el costo de reemplazar el dispositivo.

### **P. Intimidación:**

Intimidación mediante el uso de tecnología o cualquier comunicación electrónica, incluida, entre otras, la transferencia de signos, señales, escritura, imágenes, sonidos, datos o inteligencia de cualquier naturaleza transmitida por el uso de cualquier dispositivo electrónico, incluidos, pero no limitado a, una computadora, teléfono, teléfono celular, dispositivo de mensajes de texto y asistente digital personal están prohibidos.

### **Estas acciones están prohibidas:**

Se ha profundizado en la seguridad en la red, tema también dirigido por la Agencia de regulación y control de las telecomunicaciones de la República del Ecuador. El Liceo Panamericano Centenario detalla riesgos más significativos y peligrosos que se encuentran:

- ✓ **Mobbing cibernético infantil:** El acoso escolar mediante redes sociales cibernéticas, y de la internet son algo latente entre niños, niñas y adolescentes, estos inclusive pueden desencadenar suicidios de estudiantes, los cuales aún no han formado su personalidad y toma de decisiones en la vida.
- ✓ **Tráfico sexual de niños, niñas y adolescentes:** Esta es una red extensa en el mundo, y por la pesca a nivel de internet es muy usado. Estos peligros de secuestrar a nuestros estudiantes para después venderlo sean para actos sexuales o venta de órganos es algo que debemos proteger y con mucha atención.
- ✓ **Phishing Inverso Social:** Es un método muy utilizado, para escalar a través de nuestros estudiantes hacia nosotros adultos, quienes por motivos diversos quieren secuestrar, borrar o afectar significativamente nuestra integridad en la internet.
- ✓ **Phishing:** también llamado suplantación de identidad, es un tipo de delito informático que implica el intento de adquirir información confidencial de forma fraudulenta, como contraseñas, datos de tarjetas de crédito u otra información bancaria.
- ✓ **Sextorsión:** se refiere a una forma de explotación sexual en la que una persona es chantajeada con el fin de que entregue más imágenes eróticas o pornográficas, tenga relaciones sexuales con alguien o entregue dinero, bajo la amenaza de difundir imágenes previamente obtenidas de la persona realizando actos sexuales o desnuda. La víctima es condicionada a cumplir con las exigencias del chantajista para evitar la difusión de las imágenes originales.
- ✓ **Stalking:** consiste en el hostigamiento constante a una víctima, ya sea para demostrar interés amoroso o para controlar sus movimientos. También se refiere a un trastorno en



el que una persona espía a otra. El cyberstalking se produce principalmente en redes sociales y servicios de mensajería instantánea, donde se puede acceder fácilmente a la información personal de la víctima. Aunque en algunos lugares del mundo el acoso no se considera un delito, se convierte en un problema cuando se vuelve repetitivo, como el envío constante de mensajes o correos electrónicos a la víctima.

- ✓ **Harassment:** es un término que significa "acoso" o "hostigamiento" y se refiere a una conducta constante de denigrar, amenazar o insultar a alguien a través de medios electrónicos como correos electrónicos o mensajes de texto. Esto puede incluir poner apodos, difundir rumores o enviar fotos humillantes para que otros las comenten agresivamente y las reenvíen
- ✓ **Flaming:** Es el acto de insultar masivamente a un usuario en salones y/o grupos de chat.
- ✓ **Sexting:** se refiere al envío de mensajes con contenido sexual, erótico o pornográfico a través de teléfonos móviles, generalmente creados por el remitente. Esta práctica en sí misma no es dañina, pero puede volverse peligrosa si las imágenes o videos se comparten sin el consentimiento de la persona retratada. En el caso de los NNA, compartir este tipo de material sin su consentimiento constituye una grave violación de sus derechos, e incluso puede considerarse pornografía infantil.

Los avances tecnológicos han facilitado la interacción social. Estos las redes sociales y las aplicaciones móviles permiten que el contenido explícito de fotos y videos tenga gran impacto.

- **Hacking:** es una acción que consiste en manipular el funcionamiento normal de un equipo y sus sistemas conectados. Cuando se realiza de manera ilegal, implica el desbloqueo de contraseñas y códigos para obtener beneficios económicos a partir de la información obtenida.
- **Violación a la intimidad:** se refiere a la acción de fotografiar, grabar o recibir contenido audiovisual íntimo sin el consentimiento de la persona afectada y su posterior difusión a través de redes sociales como publicaciones, chats privados o grupales, entre otros. Esta acción se encuentra regulada en los artículos 103 y 178 del COIP.
- **Trata de imágenes personales:** se produce cuando se copian las fotos y videos de una persona de sus perfiles en redes sociales y se venden en línea sin su consentimiento. Estas imágenes pueden ser utilizadas en sitios pornográficos u ofrecidas para secuestrar a adolescentes con fines de explotación sexual.
- **Grooming:** se refiere a una situación en la que un adulto se hace pasar por un menor de edad en línea con el objetivo de obtener imágenes o videos de contenido sexual o erótico de la víctima, y luego utilizarlos para chantajear a la víctima y obtener favores sexuales o cometer otros delitos (Pantallas Amigas, 2019). El adulto que comete el delito (conocido como "groomer") suele aprovechar el anonimato en línea para crear identidades falsas y engañar a los NNA con los que establece vínculos emocionales.
- **Lolicon y Shotacon:** son términos utilizados para referirse a la representación o contenido de medios visuales (tales como anime, manga, videojuegos) que presentan a personajes menores de edad involucrados en relaciones sentimentales y/o sexuales con personajes adultos. Esta representación se realiza a través de la red y puede ser considerada como una forma de violencia sexual virtual.
- **Captación para trata:** se da cuando se contacta, seduce, rapta y, posteriormente, obliga a estudiantes a trabajar sexualmente, vender drogas o incluso sus órganos.
- **Ciberacoso:** se refiere a la repetida y deliberada agresión psicológica de una persona a otra utilizando dispositivos móviles o digitales para difundir mensajes,



fotos o videos que denigran y afectan la dignidad de la víctima.

## Procedimientos.

Ante una posible situación de mal uso de redes sociales, y/o situaciones antes mencionadas, se debe instar a los estudiantes a comunicar la situación con un adulto de su confianza, preferentemente, avisar de inmediato a un colaborador.

- Si un estudiante ha visto una situación donde otro compañero, que no realice un uso adecuado de las redes sociales se debe informar a un adulto de confianza para poder dar el seguimiento requerido.
- Cuando un estudiante reporte una acción anteriormente mencionada hacia su persona o la de otro compañero, se mantendrá el anonimato hasta donde sea posible para resguardar su integridad y bienestar.

Se debe instar a los estudiantes a defenderse de cualquier forma de violencia a través del establecimiento de límites claros y firmes, sin llegar a ser violentos con quienes los ofenden. Debido a que el colegio busca fomentar la resolución de conflictos de manera asertiva y en conjunto con los valores del mismo, si un estudiante se defiende de una ofensa física o verbal de manera violenta, podrá ser acreedor a una consecuencia disciplinaria.

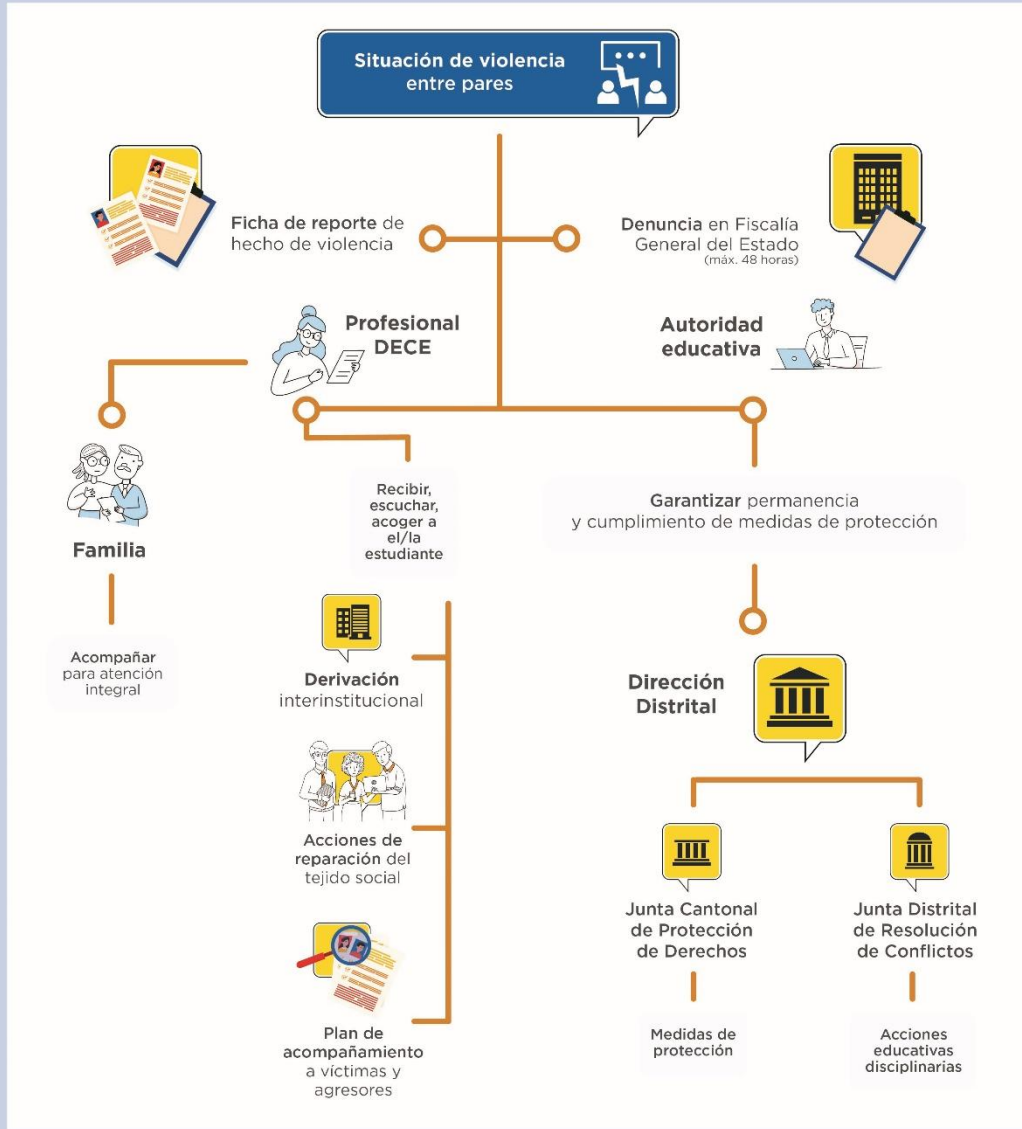
- Cuando el colegio reciba una denuncia de un posible caso de cyberbullying, entre otro tipo de violencia en línea se debe referir el caso al departamento de Consejería Estudiantil y Líder de Salvaguarda. Este departamento se encargará de hacer la investigación y seguimiento pertinente, reportando la información que corresponda a las partes involucradas.
- La información relacionada al seguimiento y/o consecuencias de una situación de violencia en línea sólo será compartida con la familia del estudiante en cuestión, y el DECE. Para el resguardo del bienestar de los estudiantes, bajo ninguna circunstancia se proporcionará información del seguimiento y/o consecuencias a otros adultos y/o estudiantes.

Posterior a las decisiones que el DECE, Líder de Salvaguarda y Rectorado tomen respecto a un caso de bullying, se llevarán a cabo las acciones y/o consecuencias pertinentes. Estas acciones pueden incluir alguna consecuencia disciplinaria dependiendo el Art. 134 de la Ley Orgánica de Educación Intercultural. Además, se puede activar la ruta y protocolo correspondiente.

### ✓ Ruta de actuación frente a casos de violencia entre estudiantes

Si cualquier persona de la comunidad educativa tiene conocimiento de un presunto caso de violencia física y/o psicológica por parte de estudiantes hacia sus pares, tiene la obligación de hacer la denuncia ante la autoridad educativa institucional, quien a su vez pondrá el caso en conocimiento de la Dirección Distrital de Educación.

## Ruta frente a casos de Violencia ENTRE ESTUDIANTES



Siempre sea amable, tenga cortesía común y sea considerado con los demás. Mostrar las conductas sociales en línea que modelan una buena ciberciudadanía se enfatiza y se fomenta.

Elaborado por:	Revisado por:	Autorizado por:
Sulay Villamar. Líder Designado de Salvaguarda	Eddna Peñafiel Sarcos Directora Académica	María Auxiliadora Velarde Cevallos Rectorado