Consejo Consultivo
SIPINNA COLIMA

En colaboración con:
Red por la Ciberseguridad

Recomendaciones para la proteccion digital de niñas, niños y adolescentes en comunidades escolares

Manual práctico para escuelas de educación básica y media

Políticas, protocolos y herramientas para una convivencia digital segura



COLIMA Gobierno del Estado · SIPINNA · FGE Fiscalía General del Estado de Colima · PRONNA · Universidad de Colima · UNIVA La Universidad Católica · Universidad Multitécnica Profesional · Fundación CENDES · World Vision

Presentación

El presente documento reúne políticas y protocolos recomendados para fortalecer la protección digital de niñas, niños y adolescentes en comunidades escolares y centros educativos. Su propósito es ofrecer una guía práctica, preventiva y adaptable para promover el uso seguro, responsable y respetuoso de tecnologías digitales en la vida escolar.

Estas recomendaciones se emiten en el marco de los trabajos del Consejo Consultivo de SIPINNA Colima, con enfoque de derechos, prevención de riesgos, corresponsabilidad comunitaria, protección de datos personales, no revictimización y canalización responsable ante incidentes digitales.

Justificación

La vida escolar ocurre cada vez más en entornos físicos y digitales conectados. Las niñas, niños y adolescentes utilizan internet, plataformas educativas, redes sociales, aplicaciones de mensajería, videojuegos, dispositivos móviles y herramientas de inteligencia artificial para aprender, convivir, expresarse y comunicarse. Esta realidad amplía oportunidades educativas, pero también incrementa la exposición a riesgos como ciberacoso, violencia digital, difusión no autorizada de imágenes, suplantación de identidad, exposición de datos personales, contenidos no adecuados para la edad, fraudes, contactos de riesgo y afectaciones a la privacidad, la dignidad y el bienestar emocional.

En este contexto, las comunidades escolares y centros educativos requieren contar con criterios claros, preventivos y aplicables para orientar el uso seguro y responsable de las tecnologías digitales. La ausencia de reglas comunes, rutas de reporte, medidas de protección y mecanismos de documentación puede provocar respuestas improvisadas, exposición innecesaria de estudiantes, revictimización, pérdida de evidencias o falta de seguimiento institucional ante incidentes digitales.

Estas recomendaciones buscan fortalecer la capacidad preventiva y de respuesta de las escuelas desde un enfoque de derechos de niñas, niños y adolescentes, corresponsabilidad comunitaria, protección de datos personales, confidencialidad, no revictimización, proporcionalidad y canalización responsable. No pretenden sustituir las obligaciones legales, reglamentos internos o protocolos oficiales de cada autoridad educativa, sino ofrecer una base práctica que pueda adaptarse a la realidad de cada plantel, respetando su contexto, recursos disponibles y marco normativo aplicable.

La protección digital de niñas, niños y adolescentes no puede recaer únicamente en las familias, en las escuelas o en las plataformas tecnológicas. Requiere una respuesta coordinada entre autoridades, directivos, docentes, personal escolar, madres, padres, personas cuidadoras, estudiantes y comunidad. Por ello, este documento propone políticas, protocolos y formatos de apoyo que facilitan la prevención, la actuación oportuna y la mejora continua en materia de convivencia y seguridad digital escolar.

Emitir estas recomendaciones en el marco de los trabajos del Consejo Consultivo de SIPINNA Colima permite impulsar una visión común para que los centros educativos cuenten con

herramientas mínimas para anticipar riesgos, proteger la integridad de niñas, niños y adolescentes y promover entornos digitales seguros, respetuosos e inclusivos.

Índice

Presentación 1
Justificación 1
Naturaleza y alcance de las recomendaciones 5
Principios transversales para la protección digital escolar 5
Política de uso responsable de tecnologías digitales 6
Objetivo 6
Alcance 6
Principios de uso responsable 6
Reglas generales para toda la comunidad escolar 6
Reglas para estudiantes 7
Reglas para docentes y personal escolar 8
Reglas para madres, padres y personas cuidadoras 8
Uso de software de seguridad y software original 8
Conductas no permitidas 9
Atención ante incumplimientos 9
Responsabilidades institucionales 9
Evidencias sugeridas para la política de uso responsable 10
Formato de aceptación de la Política de Uso Responsable 10
Protocolo de prevención y atención del ciberacoso escolar 11
Objetivo 11
Alcance 11
Definición operativa de ciberacoso 11
Conductas que pueden constituir ciberacoso 11
Principios de actuación 12
Ruta de atención 12
Medidas inmediatas recomendadas 13
Roles y responsabilidades 14
Criterios de gravedad 14
Medidas educativas y restaurativas 15
Evidencias sugeridas para el protocolo de ciberacoso escolar 15
Formato breve de reporte de ciberacoso 15
Protocolo de prevención y atención de violencia digital 16
Objetivo 16

Alcance 16
Definición operativa de violencia digital 16
Diferencia entre ciberacoso y violencia digital 16
Conductas que pueden constituir violencia digital 17
Principios de actuación 17
Ruta de atención 18
Criterios de gravedad 19
Medidas de prevención 19
Medidas educativas, restaurativas y de protección 19
Evidencias sugeridas para el protocolo de violencia digital 20
Formato breve de reporte de violencia digital 20
Política de seguridad digital básica para centros educativos 21
Objetivo 21
Alcance 21
Reglas de seguridad digital básica 21
Reglas operativas mínimas 22
Responsabilidades 23
Revisión semestral de seguridad básica 23
Evidencias sugeridas de seguridad digital básica 24
Formatos de apoyo sugeridos 24
Protocolo de prevención y actuación ante difusión no autorizada de imágenes, videos o información sensible de estudiantes 25
Objetivo 25
Alcance 25
Principios de actuación 25
Conductas o situaciones que activa el protocolo 26
Ruta de actuación 26
Medidas inmediatas recomendadas 27
Criterios de gravedad 27
Prevención 28
Responsabilidades 28
Evidencias de cumplimiento 29
Formato breve de reporte 29

Naturaleza y alcance de las recomendaciones

Estas recomendaciones buscan servir como base práctica para que comunidades escolares y centros educativos adopten, adapten o fortalezcan políticas y protocolos de seguridad digital escolar. No sustituyen disposiciones legales, lineamientos oficiales, reglamentos internos, protocolos institucionales ni obligaciones establecidas por las autoridades competentes.

Cada centro educativo podrá adaptar estas recomendaciones conforme a su contexto, nivel educativo, recursos disponibles, estructura interna, canales de comunicación, normas de convivencia y marco normativo aplicable. Su implementación debe realizarse con enfoque preventivo, gradual, documentado y proporcional, privilegiando siempre la protección de niñas, niños y adolescentes.

Cuando una situación implique riesgo grave, posible conducta ilícita, afectación significativa a la integridad, privacidad o bienestar de una niña, niño o adolescente, o exceda las capacidades de actuación del centro educativo, deberá realizarse la canalización correspondiente a las autoridades o instancias competentes.

Principios transversales para la protección digital escolar

- Interés superior de niñas, niños y adolescentes.
- Protección inmediata ante riesgos o incidentes digitales.
- Confidencialidad y manejo responsable de información sensible.
- No revictimización de la persona afectada.
- Mínima exposición de datos personales, imágenes, videos o evidencias.
- Proporcionalidad en las medidas educativas, preventivas y de atención.
- Preservación segura de evidencia sin amplificar el daño.
- Canalización responsable cuando exista riesgo grave o posible conducta ilícita.
- Enfoque educativo, restaurativo y preventivo.
- Mejora continua mediante revisión, documentación y seguimiento.

Política de uso responsable de tecnologías digitales

La presente Política de Uso Responsable de Tecnologías Digitales establece reglas claras para el uso adecuado, seguro, respetuoso y responsable de internet, computadoras, dispositivos, plataformas, cuentas, redes y servicios digitales vinculados a la vida escolar. Su finalidad es orientar a la comunidad educativa en la prevención de riesgos digitales y en la protección de niñas, niños y adolescentes.

Objetivo

Establecer criterios mínimos para que estudiantes, docentes, personal administrativo, madres, padres, personas cuidadoras y terceros autorizados utilicen las tecnologías digitales de la escuela de manera segura, ética, legal, respetuosa y alineada con la protección de niñas, niños y adolescentes.

Alcance

Esta política aplica al uso de equipos de cómputo, tabletas, dispositivos móviles, redes WiFi, plataformas educativas, correo institucional, aplicaciones de mensajería, servicios en la nube, sistemas escolares, cuentas institucionales y cualquier otro medio digital utilizado para actividades escolares, administrativas, formativas o de comunicación vinculadas con la institución.

Principios de uso responsable

- Respeto a la dignidad, privacidad e integridad de todas las personas.
- Protección prioritaria de niñas, niños y adolescentes.
- Uso educativo, formativo y administrativo de los recursos digitales.
- Prevención de ciberacoso, violencia digital, discriminación y exposición indebida de datos.
- Confidencialidad de información escolar, académica, familiar y personal.
- Uso de software original, actualizado y protegido con mecanismos de seguridad.
- Responsabilidad individual por el uso de cuentas, contraseñas y dispositivos asignados.

Reglas generales para toda la comunidad escolar

Regla	Descripción	Evidencia sugerida
Uso con fines escolares	Los recursos digitales de la escuela deberán utilizarse prioritariamente para actividades educativas, administrativas, de comunicación institucional o de formación.	Política firmada o comunicada a la comunidad escolar.

Respeto en la comunicación digital	No se permitirá el uso de medios digitales para insultar, acosar, amenazar, humillar, discriminar, excluir o difundir rumores sobre cualquier integrante de la comunidad escolar.	Comunicados, reglamento interno o protocolo de convivencia digital.
Protección de datos personales	No deberán compartirse datos personales, fotografías, videos, calificaciones, expedientes, ubicaciones o información sensible sin autorización y justificación institucional.	Aviso de privacidad, reglas de uso de imagen y formatos de autorización.
Uso correcto de cuentas	Las cuentas escolares son personales o institucionales según corresponda. No deben compartirse contraseñas ni utilizar cuentas de otras personas.	Procedimiento de alta y baja de cuentas.
Software seguro y original	Los equipos escolares deberán usar software autorizado, original, actualizado y con herramientas de seguridad activas cuando aplique.	Inventario de software, licencias, capturas o evidencia de protección activa.
Navegación responsable	No se permitirá acceder, almacenar o difundir contenido ilegal, violento, discriminatorio, sexual, de odio, fraudulento o no adecuado para la edad de estudiantes.	Reglas de navegación, filtros, controles o bitácora técnica.
Resguardo de información	La información escolar relevante deberá protegerse mediante respaldos, controles de acceso y medidas básicas de seguridad.	Procedimiento de respaldo o evidencia de resguardo.
Reporte de incidentes	Cualquier incidente digital deberá reportarse al responsable escolar designado, dirección escolar o canal definido por la institución.	Bitácora de incidentes digitales.

Reglas para estudiantes

- Usar internet, equipos y plataformas únicamente para actividades autorizadas por la escuela.
- No compartir contraseñas, cuentas, fotografías, videos o información personal propia o de otras personas.
- No grabar, fotografiar o difundir contenido de compañeros, docentes o personal escolar sin autorización.

- No participar en ciberacoso, burlas, amenazas, exclusión, suplantación de identidad o difusión de contenido ofensivo.
- Reportar a una persona adulta de confianza cualquier situación de riesgo, contacto extraño, amenaza, acoso o exposición de datos.
- Usar herramientas de inteligencia artificial de forma honesta, responsable y conforme a las indicaciones docentes.

Reglas para docentes y personal escolar

- Usar canales institucionales o autorizados para comunicación escolar.
- Evitar compartir datos personales de estudiantes por medios no autorizados.
- No publicar imágenes o videos de estudiantes sin autorización institucional y criterios de protección.
- Promover actividades formativas sobre ciudadanía digital, privacidad y respeto en línea.
- Reportar incidentes digitales al responsable escolar designado o a la dirección escolar.
- Proteger cuentas, contraseñas, calificaciones, listas, expedientes y documentos escolares.

Reglas para madres, padres y personas cuidadoras

- Respetar los canales de comunicación definidos por la escuela.
- No difundir imágenes, datos o información de otros estudiantes sin autorización.
- Evitar mensajes ofensivos, intimidatorios o discriminatorios en grupos escolares o plataformas digitales.
- Reportar oportunamente incidentes digitales que involucren a estudiantes.
- Acompañar el uso de internet y tecnología en casa, reforzando las campañas de prevención de la escuela.

Uso de software de seguridad y software original

La escuela deberá promover que los equipos utilizados para actividades escolares cuenten con software original, actualizado y protegido con herramientas de seguridad adecuadas. Este requisito no busca imponer marcas o proveedores, sino asegurar que la institución reduzca riesgos de malware, pérdida de información, acceso no autorizado y exposición de datos personales.

Elemento mínimo	Descripción	Evidencia sugerida
Software original	Los equipos escolares deben evitar el uso de software pirata, no autorizado o de origen desconocido.	Inventario de software o evidencia de licenciamiento.

Protección contra malware	Los equipos deben contar con protección activa contra malware, virus, ransomware u otras amenazas comunes.	Captura de estado de protección, consola o registro de seguridad.
Actualizaciones	Sistemas y aplicaciones deben actualizarse con periodicidad razonable.	Registro, captura o checklist de actualización.
Control de instalación	La instalación de programas debe ser autorizada por la escuela o responsable técnico.	Regla interna o bitácora de instalación.
Revisión periódica	Debe realizarse al menos una revisión semestral de seguridad básica en equipos escolares.	Checklist, acta o reporte técnico.

Conductas no permitidas

- Usar recursos digitales para acosar, amenazar, humillar, discriminar o difundir rumores.
- Compartir contraseñas o acceder a cuentas ajenas.
- Grabar, fotografiar o difundir contenido de otras personas sin autorización.
- Instalar software no autorizado, pirata o de origen desconocido en equipos escolares.
- Intentar desactivar herramientas de protección, filtros o controles escolares.
- Acceder, almacenar o distribuir contenido ilegal, dañino o no adecuado para la edad de estudiantes.
- Compartir información escolar confidencial fuera de los canales autorizados.
- Usar herramientas digitales para suplantar identidad, falsificar evidencias o manipular información.

Atención ante incumplimientos

El incumplimiento de esta política deberá atenderse con enfoque educativo, preventivo, proporcional y no punitivo, priorizando la protección de niñas, niños y adolescentes. Cuando el caso implique violencia digital, ciberacoso, exposición de datos personales, riesgo para la integridad o posible conducta ilícita, deberá activarse la ruta de reporte, atención y canalización correspondiente.

Responsabilidades institucionales

Figura	Responsabilidad
Dirección escolar	Aprobar la política, comunicarla y respaldar su aplicación.

Responsable escolar designado	Coordinar su difusión, integrar evidencias y dar seguimiento a reportes.
Comité escolar o instancia designada	Revisar avances, proponer ajustes y acompañar campañas de sensibilización.
Docentes	Aplicar reglas en actividades educativas y promover uso responsable de tecnología.
Estudiantes	Usar recursos digitales de forma respetuosa, segura y conforme a las reglas.
Familias	Acompañar el uso de tecnología y respetar canales de comunicación escolar.

Evidencias sugeridas para la política de uso responsable

- Política de uso responsable aprobada por la dirección escolar.
- Acta o evidencia de comunicación de la política a docentes, estudiantes y familias.
- Inclusión de la política en el reglamento interno, expediente escolar de protección digital o carpeta de convivencia y protección digital.
- Material de difusión, circular, cartel, infografía o publicación institucional.
- Registro de capacitación o sesión informativa sobre uso responsable.
- Bitácora de incidentes vinculada a la aplicación de la política, cuando corresponda.

Formato de aceptación de la Política de Uso Responsable

Campo	Información a registrar
Nombre de la escuela	
Nombre de la persona que acepta	
Rol	Estudiante / Docente / Madre, padre o persona cuidadora / Personal administrativo / Otro
Fecha	
Manifestación de conocimiento	Declaro conocer la Política de Uso Responsable de Tecnologías Digitales y me comprometo a respetarla conforme a mi rol dentro de la comunidad escolar.
Firma	

Protocolo de prevención y atención del ciberacoso escolar

El presente Protocolo de Prevención y Atención del Ciberacoso Escolar establece una ruta clara, educativa, confidencial y proporcional para prevenir, identificar, atender, documentar y dar seguimiento a situaciones de ciberacoso que involucren a niñas, niños y adolescentes dentro del entorno escolar o en espacios digitales vinculados a la vida escolar.

Objetivo

Establecer un procedimiento institucional para prevenir y atender situaciones de ciberacoso escolar, protegiendo la dignidad, integridad, privacidad y bienestar de niñas, niños y adolescentes, sin revictimización y con enfoque de prevención, acompañamiento y mejora continua.

Alcance

Este protocolo aplica a incidentes de ciberacoso que ocurran mediante redes sociales, servicios de mensajería, plataformas educativas, correo electrónico, videojuegos, foros, imágenes, videos, publicaciones, grupos digitales o cualquier otro medio tecnológico cuando exista vínculo con la comunidad escolar, la convivencia educativa o la seguridad de estudiantes.

Definición operativa de ciberacoso

Para efectos de estas recomendaciones, se entenderá por ciberacoso cualquier conducta reiterada o significativa de hostigamiento, intimidación, humillación, amenaza, exclusión, ridiculización, difusión de rumores, exposición de información, suplantación de identidad o uso de contenido digital para afectar a una persona integrante de la comunidad escolar.

Conductas que pueden constituir ciberacoso

- Mensajes ofensivos, humillantes, intimidatorios o amenazantes.
- Difusión de rumores, burlas, memes o publicaciones dirigidas a dañar a una persona.
- Exclusión deliberada de grupos digitales con intención de aislar o humillar.
- Suplantación de identidad o creación de perfiles falsos.
- Difusión de fotografías, videos, capturas de pantalla o datos personales sin autorización.
- Hostigamiento reiterado mediante mensajes, llamadas, comentarios o etiquetas.
- Grabación o difusión de contenido de agresiones, burlas o situaciones privadas.
- Presión, chantaje o amenaza para obtener imágenes, información o acciones de una persona.

Principios de actuación

Principio	Aplicación en el protocolo
Protección inmediata	La prioridad será detener la exposición, reducir el daño y proteger a la persona afectada.
Confidencialidad	La información del caso se compartirá solo con quienes deban intervenir.
No revictimización	Se evitará culpar, exponer, confrontar innecesariamente o presionar a la persona afectada.
Enfoque educativo	La atención buscará corregir conductas, reparar daños y prevenir repetición.
Proporcionalidad	Las medidas deberán corresponder a la gravedad, reiteración, edad y contexto.
Preservación de evidencia	Se deberán conservar capturas, enlaces, fechas, usuarios y descripciones sin difundir el contenido.

Ruta de atención

Etapa	Acción	Responsable sugerido	Evidencia
1. Recepción del reporte	Recibir el reporte por canal definido, sin minimizar ni exponer a la persona afectada.	Responsable escolar designado, dirección escolar o docente designado.	Bitácora de incidentes digitales.
2. Medidas inmediatas	Proteger a la persona afectada, detener la difusión cuando sea posible y evitar confrontaciones improvisadas.	Dirección escolar y responsable escolar designado.	Registro de medidas inmediatas.
3. Preservación de evidencia	Guardar capturas, enlaces, fechas, usuarios y descripción objetiva del incidente.	Responsable escolar designado o persona autorizada.	Carpeta confidencial del caso.
4. Valoración inicial	Identificar gravedad, reiteración, personas involucradas, riesgo	Comité escolar o instancia designada, orientación o convivencia escolar.	Formato de valoración o minuta confidencial.

	emocional y necesidad de canalización.		
5. Comunicación con familias	Informar a madres, padres o personas cuidadoras cuando corresponda, con cuidado de no revelar información innecesaria.	Dirección escolar.	Registro de comunicación.
6. Plan de intervención	Definir medidas educativas, restaurativas, de acompañamiento, seguridad y seguimiento.	Dirección escolar, responsable escolar designado y comité escolar o instancia designada.	Plan de atención o Plan de mejora.
7. Canalización externa	Canalizar a instancias competentes cuando exista riesgo grave, violencia, exposición de datos o posible delito.	Dirección escolar.	Registro de canalización.
8. Seguimiento y cierre	Verificar que cesó la conducta, documentar acciones y reforzar prevención.	Responsable escolar designado y comité escolar o instancia designada.	Bitácora actualizada y reporte de cierre.

Medidas inmediatas recomendadas

- Escuchar a la persona afectada en un espacio seguro y privado.
- Evitar pedirle que repita innecesariamente lo ocurrido ante varias personas.
- Solicitar que no elimine evidencias relevantes hasta que sean registradas de forma segura.
- Evitar compartir capturas o contenidos con personas no autorizadas.
- Valorar si se requiere acompañamiento emocional, ajuste temporal de grupos digitales o apoyo familiar.
- Solicitar retiro de contenidos cuando sea viable, sin poner en riesgo adicional a la persona afectada.
- Activar rutas de canalización si existe amenaza, violencia, extorsión, exposición íntima, riesgo físico o daño emocional grave.

Roles y responsabilidades

Figura	Responsabilidad
Dirección escolar	Autorizar medidas, comunicar a familias, coordinar canalizaciones y asegurar el cumplimiento del protocolo.
Responsable escolar designado	Registrar el incidente, integrar evidencia, coordinar seguimiento y mantener confidencialidad.
Comité escolar o instancia designada	Analizar patrones, promover medidas preventivas y revisar avances sin exponer datos personales innecesarios.
Docentes	Reportar señales o incidentes, apoyar acciones educativas y evitar confrontaciones públicas.
Orientación, psicología, trabajo social o convivencia escolar	Brindar acompañamiento, valorar riesgos emocionales y sugerir medidas de apoyo.
Familias	Colaborar con la escuela, preservar evidencias, evitar difusión del contenido y acompañar a estudiantes.
Estudiantes	Reportar incidentes, evitar replicar contenido dañino y participar en acciones de prevención.

Criterios de gravedad

Nivel	Descripción	Respuesta sugerida
Bajo	Comentario aislado, burla no reiterada o conflicto digital sin exposición amplia.	Intervención educativa, diálogo orientado y seguimiento breve.
Medio	Conducta reiterada, difusión en grupo, afectación emocional o participación de varias personas.	Plan de intervención, comunicación con familias, medidas de protección y seguimiento.
Alto	Amenazas, extorsión, suplantación, difusión de datos sensibles, exposición pública o daño emocional grave.	Canalización externa, medidas inmediatas de protección y seguimiento formal.
Crítico	Riesgo físico, contenido íntimo, posible delito, autolesión, explotación o violencia grave.	Activación urgente de autoridades, protección especializada y resguardo estricto de evidencia.

Medidas educativas y restaurativas

- Sesiones de sensibilización sobre respeto, privacidad y consecuencias del ciberacoso.
- Compromisos escritos de no repetición cuando sean adecuados.
- Actividades de reparación simbólica o restaurativa, siempre que no revictimicen.
- Revisión de reglas de grupos digitales y comunicación escolar.
- Seguimiento individual o grupal con orientación escolar.
- Refuerzo de campañas de ciudadanía digital y uso responsable de tecnología.

Evidencias sugeridas para el protocolo de ciberacoso escolar

- Protocolo de ciberacoso aprobado por la dirección escolar.
- Ruta de reporte y atención comunicada a estudiantes, docentes y familias.
- Registro de capacitación o sensibilización sobre ciberacoso.
- Bitácora de incidentes digitales, cuando existan reportes.
- Directorio de canalización externa o ruta institucional de apoyo.
- Minuta del comité escolar o instancia designada sobre revisión del protocolo.
- Materiales preventivos: cartel, infografía, circular, guía o actividad escolar.

Formato breve de reporte de ciberacoso

Campo	Información a registrar
Fecha del reporte	
Persona que reporta	
Persona presuntamente afectada	
Medio digital utilizado	Red social / Mensajería / Plataforma escolar / Correo / Videojuego / Otro
Descripción objetiva del incidente	
Evidencia preservada	Captura / Enlace / Mensaje / Testimonio / Otro
Medidas inmediatas	
Canalización requerida	Sí / No / En valoración
Responsable de seguimiento	
Estatus	Abierto / En seguimiento / Cerrado

Protocolo de prevención y atención de violencia digital

El presente Protocolo de Prevención y Atención de Violencia Digital establece una ruta institucional para prevenir, identificar, documentar, atender y canalizar situaciones de violencia digital que afecten a niñas, niños, adolescentes o integrantes de la comunidad escolar. Su finalidad es reducir riesgos, proteger la dignidad y privacidad de las personas, y promover una respuesta educativa, confidencial y proporcional.

Objetivo

Establecer un procedimiento escolar para atender situaciones de violencia digital con enfoque de protección, confidencialidad, prevención, no revictimización y respeto a los derechos de niñas, niños y adolescentes.

Alcance

Aplica a hechos de violencia digital ocurridos mediante redes sociales, mensajería, plataformas educativas, correo electrónico, sitios web, aplicaciones, videojuegos, inteligencia artificial, edición de imágenes, perfiles falsos, difusión de datos, publicaciones, capturas de pantalla o cualquier otro medio tecnológico relacionado con la comunidad escolar.

Definición operativa de violencia digital

Para efectos de estas recomendaciones, se entenderá por violencia digital cualquier acción u omisión realizada mediante tecnologías de información y comunicación que afecte la dignidad, privacidad, integridad, seguridad, libertad, imagen, reputación, bienestar emocional o derechos de una persona integrante de la comunidad escolar.

Diferencia entre ciberacoso y violencia digital

Concepto	Descripción	Ejemplos
Ciberacoso	Forma de violencia digital caracterizada por hostigamiento, intimidación, humillación o agresión mediante medios digitales, especialmente cuando existe reiteración o intención de dañar.	Insultos reiterados, burlas en grupos, difusión de rumores, exclusión digital.
Violencia digital	Categoría más amplia que incluye acciones digitales que vulneran dignidad, privacidad, imagen, datos personales, seguridad o integridad, aunque no siempre sean reiteradas.	Difusión no autorizada de imágenes, suplantación, edición ofensiva con IA, exposición de datos, amenazas o extorsión.

Conductas que pueden constituir violencia digital

- Difusión de imágenes, videos, audios, capturas o datos personales sin autorización.
- Edición, manipulación o creación de imágenes, audios o videos para ridiculizar, dañar o sexualizar a una persona.
- Uso de inteligencia artificial para crear contenido ofensivo, falso, humillante o dañino.
- Suplantación de identidad, creación de perfiles falsos o uso indebido de cuentas.
- Amenazas, extorsión, chantaje o presión mediante medios digitales.
- Publicaciones que promuevan odio, discriminación, humillación o violencia contra una persona o grupo.
- Exposición de información privada, familiar, escolar, médica, académica o de ubicación.
- Difusión de contenido íntimo, sensible o degradante, real o manipulado.
- Uso de plataformas digitales para excluir, vigilar, perseguir o controlar a una persona.
- Almacenamiento o distribución de contenido dañino relacionado con estudiantes o personal escolar.

Principios de actuación

Principio	Aplicación
Protección de la persona afectada	La primera respuesta debe reducir el daño y proteger la integridad, privacidad y bienestar emocional.
Confidencialidad estricta	La información del caso no debe compartirse fuera del equipo autorizado.
No revictimización	Se evitará exponer, culpar o forzar a la persona afectada a relatar repetidamente los hechos.
Preservación segura de evidencia	Las evidencias deben registrarse sin reenviar, exhibir o amplificar el contenido dañino.
Proporcionalidad	La respuesta debe considerar gravedad, edad, contexto, reiteración y daño generado.
Canalización responsable	Cuando exista posible delito, riesgo grave o afectación significativa, se deberá canalizar a instancias competentes.

Ruta de atención

Etapa	Acción	Responsable sugerido	Evidencia
1. Recepción del reporte	Recibir la información por canal institucional, con escucha respetuosa y sin minimizar el hecho.	Responsable escolar designado, dirección escolar o persona designada.	Bitácora de incidentes digitales.
2. Protección inmediata	Adoptar medidas para reducir exposición, impedir difusión adicional y proteger a la persona afectada.	Dirección escolar y responsable escolar designado.	Registro de medidas inmediatas.
3. Resguardo de evidencia	Preservar capturas, enlaces, perfiles, fechas, usuarios y descripciones objetivas sin difundir el contenido.	Responsable escolar designado o persona autorizada.	Carpeta confidencial del caso.
4. Valoración de gravedad	Identificar tipo de violencia, alcance, personas involucradas, riesgo, daño emocional y necesidad de canalización.	Dirección escolar, responsable escolar designado, orientación o convivencia escolar.	Formato de valoración o minuta confidencial.
5. Comunicación institucional	Informar a madres, padres o personas cuidadoras cuando corresponda, cuidando privacidad y datos sensibles.	Dirección escolar.	Registro de comunicación.
6. Plan de atención	Definir medidas educativas, preventivas, disciplinarias institucionales, restaurativas o de apoyo, según el caso.	Dirección escolar, responsable escolar designado y comité escolar o instancia designada.	Plan de mejora o plan de atención.
7. Canalización externa	Canalizar cuando exista contenido íntimo, amenazas, extorsión, riesgo físico, posible delito o daño grave.	Dirección escolar.	Registro de canalización.
8. Seguimiento y prevención	Verificar cierre, evitar represalias, actualizar medidas preventivas y reforzar campañas.	Responsable escolar designado y comité escolar o instancia designada.	Bitácora actualizada, minuta o reporte de cierre.

Criterios de gravedad

Nivel	Descripción	Respuesta sugerida
Bajo	Uso inadecuado aislado sin difusión amplia ni afectación grave.	Orientación educativa, retiro voluntario del contenido y seguimiento.
Medio	Difusión en grupo, afectación emocional, reiteración o participación de varias personas.	Plan de atención, comunicación con familias, medidas de protección y seguimiento.
Alto	Suplantación, amenazas, exposición de datos sensibles, edición dañina, difusión pública o daño significativo.	Canalización externa, medidas formales de protección y seguimiento documentado.
Crítico	Contenido íntimo, extorsión, riesgo físico, posible delito, explotación, autolesión o violencia grave.	Activación urgente de autoridades competentes y atención especializada.

Medidas de prevención

- Campañas periódicas sobre violencia digital, privacidad, consentimiento y huella digital.
- Sesiones para estudiantes sobre uso responsable de imágenes, inteligencia artificial y redes sociales.
- Talleres para familias sobre acompañamiento digital y señales de alerta.
- Capacitación docente para identificar y reportar incidentes.
- Reglas claras para grupos de mensajería, plataformas escolares y publicación de imágenes.
- Promoción de canales de reporte seguros, confidenciales y accesibles.

Medidas educativas, restaurativas y de protección

- Retiro o solicitud de retiro de contenido, cuando sea viable y seguro.
- Compromisos de no repetición y actividades de sensibilización.
- Acompañamiento emocional o canalización psicosocial cuando se requiera.
- Revisión de permisos, cuentas, grupos o canales digitales utilizados.
- Medidas de separación digital temporal cuando exista riesgo de reiteración.
- Acciones de reparación simbólica, siempre que no generen revictimización.

Evidencias sugeridas para el protocolo de violencia digital

- Protocolo de violencia digital aprobado por la dirección escolar.
- Evidencia de difusión del protocolo a docentes, estudiantes y familias.
- Ruta de reporte y canalización visible o comunicada.
- Registro de capacitación o sensibilización sobre violencia digital.
- Bitácora de incidentes digitales, cuando existan reportes.
- Directorio de canalización externa o ruta institucional de apoyo.
- Material preventivo sobre privacidad, consentimiento, violencia digital e inteligencia artificial.
- Minuta del comité escolar o instancia designada sobre revisión del protocolo.

Formato breve de reporte de violencia digital

Campo	Información a registrar
Fecha del reporte	
Persona que reporta	
Persona presuntamente afectada	
Tipo de violencia digital	Difusión de imagen / Suplantación / Amenaza / Exposición de datos / IA manipulada / Otro
Medio digital utilizado	Red social / Mensajería / Plataforma escolar / Correo / Sitio web / Otro
Descripción objetiva del incidente	
Evidencia preservada	Captura / Enlace / Perfil / Mensaje / Testimonio / Otro
Medidas inmediatas	
Canalización requerida	Sí / No / En valoración
Responsable de seguimiento	
Estatus	Abierto / En seguimiento / Cerrado

Política de seguridad digital básica para centros educativos

La presente Política de Seguridad Digital Básica para Centros Educativos establece medidas mínimas para proteger equipos, cuentas, redes, información escolar, plataformas y servicios digitales utilizados por la comunidad educativa. Su finalidad es reducir riesgos tecnológicos y fortalecer prácticas básicas de seguridad digital en centros educativos.

Objetivo

Establecer medidas básicas, verificables y proporcionales para reducir riesgos de acceso no autorizado, pérdida de información, malware, uso indebido de cuentas, navegación insegura y exposición de datos personales en los recursos tecnológicos de la escuela.

Alcance

Esta política aplica a computadoras, tabletas, dispositivos móviles institucionales, redes WiFi, cuentas institucionales, plataformas educativas, sistemas administrativos, servicios en la nube, respaldos, software instalado, herramientas de seguridad y cualquier recurso TIC utilizado para actividades escolares o administrativas.

Reglas de seguridad digital básica

No.	Regla	Requisito mínimo	Evidencia sugerida
1	Inventario de equipos	La escuela deberá mantener un inventario actualizado de equipos usados para actividades escolares o administrativas.	Inventario con ubicación, responsable, estado y uso principal.
2	Control de acceso a equipos	Los equipos deberán contar con reglas de acceso, usuarios definidos o responsables asignados.	Listado de usuarios, bitácora de préstamo o reglas de acceso.
3	Contraseñas robustas	Las cuentas institucionales deberán usar contraseñas seguras, no compartidas y cambiadas cuando exista riesgo.	Política de contraseñas, circular o evidencia de comunicación.
4	Software de seguridad y software original	Los equipos deberán usar software autorizado, original y con protección activa contra amenazas comunes.	Inventario, licencia, captura de protección activa o consola de seguridad.

5	Actualización periódica	Sistemas, navegadores, aplicaciones y herramientas de seguridad deberán actualizarse con periodicidad razonable.	Checklist, capturas o reporte de actualización.
6	Respaldo de información	La información crítica escolar deberá respaldarse de forma periódica y resguardarse con acceso controlado.	Procedimiento de respaldo, registro o evidencia de copia.
7	Uso seguro de red WiFi	La red WiFi deberá contar con contraseña, reglas de uso y, cuando sea posible, separación entre red administrativa, docente, estudiantil o de invitados.	Reglas de red, configuración, cartel interno o reporte técnico.
8	Filtro o reglas de navegación	La escuela deberá establecer reglas o mecanismos para reducir el acceso a contenidos no adecuados para estudiantes.	Reglas de navegación, filtro, control parental, proxy o política comunicada.
9	Cuenta institucional administrada	Las cuentas escolares deberán tener responsable de administración, reglas de alta, baja y recuperación.	Procedimiento de administración de cuentas o listado de responsables.
10	Reporte técnico de incidentes	Los incidentes técnicos deberán registrarse y atenderse mediante un canal definido.	Formato de reporte técnico, bitácora o correo de seguimiento.
11	Revisión semestral de controles	La escuela deberá revisar al menos dos veces por ciclo escolar el estado de sus controles básicos de seguridad.	Checklist semestral, acta o reporte técnico.

Reglas operativas mínimas

- No instalar software pirata, no autorizado, de origen desconocido o que no tenga finalidad escolar.
- No desactivar antivirus, protección contra malware, filtros o controles definidos por la escuela.
- No compartir cuentas, contraseñas o accesos administrativos.
- No usar equipos escolares para descargar contenido ilegal, dañino o no adecuado para estudiantes.
- No conectar dispositivos externos desconocidos sin autorización o revisión previa.

- No almacenar información sensible sin control de acceso o respaldo adecuado.
- Reportar fallas, alertas, infecciones, pérdida de equipo, accesos sospechosos o incidentes técnicos.
- Separar, cuando sea posible, el uso administrativo, docente, estudiantil y de invitados.

Responsabilidades

Figura	Responsabilidad
Dirección escolar	Aprobar la política, asignar responsables y respaldar su cumplimiento.
Responsable escolar designado	Integrar evidencias, coordinar revisión semestral y dar seguimiento a hallazgos.
Responsable de tecnología o soporte	Apoyar inventario, actualizaciones, respaldos, software de seguridad, red WiFi y reportes técnicos.
Docentes y personal administrativo	Usar cuentas y equipos de forma segura, reportar incidentes y proteger información escolar.
Estudiantes	Usar equipos y redes conforme a las reglas definidas y reportar situaciones de riesgo.
Familias	Reforzar el uso seguro de dispositivos y cuentas cuando existan actividades escolares desde casa.

Revisión semestral de seguridad básica

La escuela deberá realizar una revisión semestral de controles básicos para verificar el avance en las medidas de seguridad digital. Esta revisión no requiere herramientas avanzadas, pero sí evidencia documental y seguimiento de hallazgos.

Control revisado	Cumple	Parcial	No cumple	Hallazgo / acción requerida
Inventario de equipos actualizado				
Control de acceso a equipos				
Contraseñas robustas comunicadas				

Software original y protección activa				
Actualizaciones revisadas				
Respaldos definidos o ejecutados				
Red WiFi con reglas de uso				
Reglas o filtros de navegación				
Cuentas institucionales administradas				
Canal de reporte técnico				
Plan de mejora derivado de revisión				

Evidencias sugeridas de seguridad digital básica

- Política de seguridad digital básica para centros educativos aprobada y comunicada.
- Inventario de equipos, plataformas, cuentas y software relevante.
- Evidencia de software original o autorizado y protección activa en equipos escolares.
- Reglas de contraseñas, acceso a equipos y administración de cuentas.
- Procedimiento o evidencia de respaldos de información escolar crítica.
- Reglas de uso de red WiFi y navegación segura.
- Formato o bitácora de reporte técnico de incidentes.
- Checklist semestral de revisión de controles y plan de mejora cuando aplique.

Formatos de apoyo sugeridos

Formato	**Uso relacionado**
Autoevaluación inicial	Identificar brechas en seguridad digital básica.
Plan de mejora	Dar seguimiento a hallazgos técnicos o controles pendientes.
Acta de revisión documental o visita	Registrar revisión de evidencias de seguridad básica.
Bitácora de incidentes digitales	Registrar incidentes digitales vinculados con equipos, cuentas, plataformas o red.
Inventario básico de servicios digitales	Registrar plataformas, servicios, responsables, controles y riesgos observados.

Protocolo de prevención y actuación ante difusión no autorizada de imágenes, videos o información sensible de estudiantes

El presente protocolo establece una ruta institucional para prevenir, atender y dar seguimiento a la difusión no autorizada de imágenes, videos, audios, capturas de pantalla, datos personales o cualquier información sensible de estudiantes. Su enfoque es de protección, privacidad, no revictimización, confidencialidad y canalización responsable.

Objetivo

Establecer medidas preventivas y una ruta de actuación para proteger a niñas, niños y adolescentes ante la difusión no autorizada de contenido o información sensible, reduciendo daños, evitando la revictimización y asegurando el resguardo adecuado de evidencias.

Alcance

Aplica a situaciones que involucren imágenes, videos, audios, capturas, perfiles, publicaciones, mensajes, datos personales, información familiar, académica, médica, de ubicación o cualquier contenido sensible relacionado con estudiantes, difundido o almacenado sin autorización en medios digitales vinculados directa o indirectamente con la comunidad escolar.

Principios de actuación

Principio	**Aplicación**
Protección inmediata	La prioridad será detener o reducir la difusión y proteger a la persona afectada.
No revictimización	No se culpabilizará, expondrá ni confrontará innecesariamente a la persona afectada.
Confidencialidad	La información del caso solo será conocida por quienes deban intervenir.
Resguardo seguro de evidencia	Las evidencias se preservarán sin reenviar, exhibir o ampliar la difusión del contenido.
Canalización responsable	Cuando exista riesgo, daño grave o posible conducta ilícita, se activarán rutas externas competentes.
Enfoque educativo y preventivo	Se reforzarán acciones de sensibilización sobre privacidad, consentimiento, respeto y huella digital.

Conductas o situaciones que activa el protocolo

- Publicación o reenvío de fotografías, videos, audios o capturas de estudiantes sin autorización.
- Difusión de datos personales, ubicaciones, información familiar, académica, médica o sensible.
- Uso de imágenes o datos de estudiantes para burla, humillación, amenaza, chantaje, discriminación o exposición pública.
- Creación o modificación de contenido digital que afecte la dignidad, imagen o privacidad de una persona estudiante.
- Uso de inteligencia artificial u otras herramientas para manipular imágenes, audios o videos de estudiantes con fines dañinos.
- Conservación, envío o circulación de contenido sensible en grupos escolares, redes sociales, plataformas o dispositivos.
- Negativa a retirar contenido sensible cuando la escuela o la persona afectada lo solicita por una vía razonable.

Ruta de actuación

Etapa	Acción	Responsable sugerido	Evidencia
1. Recepción del reporte	Recibir el reporte de forma respetuosa, privada y sin minimizar la situación.	Responsable escolar designado, dirección escolar o persona designada.	Bitácora de incidentes digitales.
2. Protección inmediata	Reducir exposición, evitar difusión adicional y proteger a la persona afectada.	Dirección escolar y responsable escolar designado.	Registro de medidas inmediatas.
3. Resguardo de evidencia	Preservar información mínima necesaria: fecha, medio, usuario, enlace, captura o descripción objetiva, sin reenviar el contenido.	Responsable escolar designado o persona autorizada.	Carpeta confidencial del caso.
4. Valoración de riesgo	Identificar alcance, gravedad, reiteración, edad de personas involucradas, daño emocional y necesidad de canalización.	Dirección escolar, orientación, convivencia escolar o comité escolar o instancia designada.	Formato de valoración o minuta confidencial.

5. Solicitud de retiro o contención	Solicitar retiro del contenido cuando sea viable y seguro; evitar mensajes que agraven la exposición.	Dirección escolar o persona autorizada.	Registro de solicitud o medida de contención.
6. Comunicación con familias	Informar a madres, padres o personas cuidadoras cuando corresponda, cuidando privacidad y evitando detalles innecesarios.	Dirección escolar.	Registro de comunicación.
7. Canalización externa	Canalizar a instancias competentes cuando exista riesgo grave, amenaza, exposición de datos sensibles, violencia o posible conducta ilícita.	Dirección escolar.	Registro de canalización.
8. Seguimiento y cierre	Verificar que cesó la difusión, actualizar medidas preventivas y documentar cierre.	Responsable escolar designado y comité escolar o instancia designada.	Reporte de cierre y plan de mejora, si aplica.

Medidas inmediatas recomendadas

- Escuchar a la persona afectada en un espacio seguro, privado y con acompañamiento adecuado.
- Evitar que la persona afectada muestre el contenido frente a múltiples personas.
- No reenviar, proyectar, imprimir, circular o almacenar innecesariamente el contenido sensible.
- Registrar únicamente la evidencia mínima necesaria para documentar el caso.
- Solicitar apoyo familiar o especializado cuando exista afectación emocional.
- Evitar confrontaciones públicas entre estudiantes o familias.
- Revisar si existen riesgos adicionales de represalia, burla, aislamiento o nueva difusión.

Criterios de gravedad

Nivel	Descripción	Respuesta sugerida
Bajo	Difusión limitada, sin datos sensibles y con posibilidad de retiro inmediato.	Retiro, orientación educativa y seguimiento breve.

Medio	Difusión en grupo escolar, afectación emocional o contenido personal no autorizado.	Plan de atención, comunicación con familias y seguimiento documentado.
Alto	Difusión pública, datos sensibles, manipulación de contenido, amenazas o daño significativo.	Medidas formales de protección, canalización externa y seguimiento estricto.
Crítico	Riesgo físico, extorsión, violencia grave, posible delito, explotación o afectación severa a la integridad.	Activación urgente de autoridades competentes y atención especializada.

Prevención

- Integrar reglas claras sobre uso de imagen, videos y datos personales en la política de uso responsable de tecnologías digitales.
- Solicitar autorizaciones cuando corresponda para difusión institucional de imágenes o videos.
- Capacitar a estudiantes sobre privacidad, consentimiento, huella digital y consecuencias de reenviar contenido sensible.
- Capacitar a docentes y familias sobre señales de alerta, canales de reporte y manejo de evidencias.
- Evitar publicar información que identifique innecesariamente a estudiantes.
- Establecer reglas para grupos de mensajería, redes sociales y plataformas escolares.
- Promover el mensaje: “Si afecta la privacidad o dignidad de alguien, no lo compartas”.

Responsabilidades

Figura	Responsabilidad
Dirección escolar	Autorizar medidas, comunicar a familias y coordinar canalización externa cuando sea necesario.
Responsable escolar designado	Registrar el caso, resguardar evidencia mínima, coordinar seguimiento y mantener confidencialidad.
Comité escolar o instancia designada	Revisar medidas preventivas, fortalecer campañas y analizar patrones sin exponer datos personales.
Docentes	Reportar incidentes, reforzar prevención y evitar difusión de contenido sensible.
Familias	Acompañar a estudiantes, preservar evidencia sin difundirla y colaborar con la escuela.
Estudiantes	No compartir contenido no autorizado, reportar incidentes y evitar replicar materiales dañinos.

Evidencias de cumplimiento

- Protocolo aprobado y comunicado a la comunidad escolar.
- Reglas de uso de imagen y datos personales integradas al reglamento interno, política de uso responsable o carpeta de convivencia y protección digital.
- Material de prevención sobre privacidad, consentimiento y no difusión de contenido sensible.
- Registro de capacitación o sensibilización para estudiantes, docentes y familias.
- Bitácora de incidentes digitales cuando existan incidentes.
- Formato de reporte y seguimiento de casos.
- Minuta del comité escolar o instancia designada sobre revisión de medidas preventivas.

Formato breve de reporte

Campo	Información a registrar
Fecha del reporte	
Persona que reporta	
Persona presuntamente afectada	
Tipo de contenido o información difundida	Imagen / Video / Audio / Captura / Datos personales / Información sensible / Otro
Medio digital utilizado	Red social / Mensajería / Plataforma escolar / Correo / Sitio web / Otro
Descripción objetiva del incidente	
Evidencia mínima preservada	Captura / Enlace / Perfil / Mensaje / Testimonio / Otro
Medidas inmediatas adoptadas	
Solicitud de retiro o contención	Sí / No / En valoración
Canalización requerida	Sí / No / En valoración
Responsable de seguimiento	
Estatus	Abierto / En seguimiento / Cerrado