



GUÍA ORIENTATIVA DE NORMAS Y LEYES PARA LOS EDAYO

Cómo prevenir, detectar y actuar ante riesgos y violencias digitales

Material de apoyo para el 2.º Coloquio de Ciberseguridad 2026

1 | Principio de actuación

La escuela debe prevenir, detectar, proteger, registrar, orientar, derivar y acompañar. No sustituye a la Justicia, la Policía ni a profesionales de salud. Ante una situación, actuar de manera proporcional al riesgo, preservar la confidencialidad y evitar la revictimización.

2 | Qué debe preparar cada institución ANTES de un incidente

- Designar referentes y suplentes (dirección + EDAYO); definir canales de aviso seguros y quién decide cada derivación.
- Incorporar convivencia y ciudadanía digital a acuerdos institucionales y actividades de aula: ciberacoso, grooming, IA/deepfakes, imágenes íntimas, apuestas, fraude y privacidad.
- Capacitar a docentes, preceptores, personal y familias para reconocer señales y comunicar incidentes sin exponer a estudiantes.
- Disponer de una ficha de registro reservada, acceso restringido y procedimiento para conservar evidencia de forma proporcional.
- Construir y actualizar un directorio local de contactos: dirección, SPEPM, protección de niñez, salud, Fiscalía y Policía/Cibercrimen.
- Realizar al menos un simulacro de mesa por año y revisar procedimientos después de cada situación.

3 | Ruta de actuación ante una situación

Ante un incidente: actuación básica

**ESCUCHAR Y CONTENER → PROTEGER → INFORMAR A DIRECCIÓN →
REGISTRAR SIN DIFUNDIR → EVALUAR Y DERIVAR → ACOMPAÑAR Y
HACER SEGUIMIENTO.**

Ante grooming, sextorsión, amenazas graves o material de abuso sexual infantil: activar de inmediato el protocolo y los organismos competentes. No confrontar al presunto agresor ni investigar por cuenta propia. No reenviar ni reproducir material íntimo de menores.



PASO	QUÉ HACER	QUÉ EVITAR
1. Recibir y contener	Escuchar sin juzgar; priorizar seguridad y necesidades inmediatas.	Culpar, prometer secreto absoluto o pedir relatos reiterados.
2. Proteger	Detener exposición dentro de las posibilidades de la escuela; evaluar urgencia.	Confrontar al presunto agresor o improvisar mediaciones en casos graves.
3. Informar	Activar dirección y referentes EDAYO según protocolo.	Resolver el caso en soledad o compartirlo en grupos informales.
4. Registrar	Anotar fecha, relato inicial, personas intervinientes, acciones y decisiones.	Copiar o reenviar material sensible sin necesidad.
5. Evaluar y derivar	Distinguir riesgo bajo/medio/alto; activar organismos competentes cuando corresponda.	Investigar penalmente o retrasar una derivación urgente.
6. Acompañar	Plan de seguimiento, protección de la trayectoria escolar y revisión de medidas.	Dar el caso por cerrado apenas desaparece el contenido.

4 | Niveles orientativos de respuesta

BAJO	Conflicto digital sin señales de delito, peligro inmediato ni grave vulneración: abordaje educativo, preventivo y seguimiento.
MEDIO	Daño persistente, difusión, hostigamiento o afectación relevante: activar protocolo, dirección, EDAYO, familias cuando sea seguro y articulación especializada.
ALTO / URGENTE	Grooming, sextorsión, amenazas graves, riesgo autolesivo, abuso o material sexual de menores: protección inmediata y contacto con autoridades/servicios competentes. Si hay peligro inmediato, emergencias.



5 | Qué hacer según el incidente

SITUACIÓN	PREVENIR	ACTUAR
Ciberacoso / hostigamiento	Acuerdos de convivencia, respeto, canales de aviso.	Contener; registrar sin exponer; frenar hostigamiento; evaluar gravedad y seguimiento.
Grooming / sextorsión	Charlas por edades; señales de manipulación; familias informadas.	No confrontar ni negociar; proteger; avisar a dirección; derivación urgente según protocolo.
Fotos íntimas / deepfakes con IA	Consentimiento, huella digital, prohibición de difusión y educación crítica en IA.	Evitar nueva circulación; resguardar datos mínimos; acompañar; evaluar protección y denuncia.
Apuestas online / desafíos peligrosos	Educación sobre riesgos, señales de alerta y participación familiar.	Escucha y evaluación; intervención interdisciplinaria; derivación a salud/protección si procede.
Suplantación / robo de cuentas / phishing	Contraseñas robustas, doble factor, verificación de enlaces.	Asegurar cuentas con apoyo técnico; registrar incidente; informar a afectados y evaluar exposición de datos.
Amenazas o riesgos de autolesión	Clima de confianza, detección temprana, orientación.	Priorizar seguridad y atención de salud; no dejar sola a la persona si hay peligro inmediato; activar emergencia.

6 | Normas que respaldan estas acciones

MISIONES	APLICACIÓN EDUCATIVA
Ley II N.º 42 (2026)	Prevención, detección, actuación y acompañamiento ante riesgos y violencias digitales; responsabilidades de instituciones públicas y privadas; registro y articulación.
Resolución ministerial 158/2026 y adhesión SPEPM	Protocolo provincial de actuación: prevención, niveles de riesgo, roles, resguardo de evidencia, derivaciones y seguimiento.
Ley II N.º 16	Sistema provincial de protección integral de niñas, niños y adolescentes.



Ley VI N.º 250

Abordaje, prevención y erradicación del acoso contra niñas, niños y adolescentes.

Resolución SPEPM 145/2025

Lineamientos para la conformación de los equipos EDAYO.

NACIÓN	APLICACIÓN EDUCATIVA
Ley 26.061	Derechos de niñas, niños y adolescentes; interés superior, intimidad y protección integral.
Ley 26.904 + Ley 27.590 (Mica Ortega)	Delito de grooming (art. 131 CP) y prevención/capacitación sobre grooming.
Ley 27.736 (Olimpia) + Ley 26.485	Violencia digital contra las mujeres, incluidos materiales íntimos reales o editados difundidos sin consentimiento; protección y medidas judiciales.
Ley 25.326	Protección de datos personales: confidencialidad, finalidad y acceso restringido.
Leyes 26.892, 26.150 y 26.388	Convivencia escolar, educación sexual integral y delitos informáticos.

7 | Advertencias que deben recordarse

- No toda conducta dañina en internet es automáticamente delito: la escuela igualmente debe evaluar y actuar dentro de sus competencias.
- No descargar, reenviar ni reproducir material sexual de menores. Preservar identificadores, enlaces y datos pertinentes siguiendo indicaciones de la autoridad competente.
- La comunicación con familias debe considerar la seguridad de la persona afectada y el protocolo; no divulgar nombres ni detalles en comunicaciones generales.
- La Ley Olimpia no crea por sí sola un delito penal para toda imagen falsa: incorpora la violencia digital de género al marco de protección de la Ley 26.485.

8 | Control rápido para cada

EDAYO ☐ ¿Tenemos referente y suplente?

☐ ¿Sabemos a quién llamar ante riesgo alto?

☐ ¿Tenemos ficha reservada y procedimiento de evidencia?

☐ ¿Se capacitó al personal y se informó a las familias?

☐ ¿Existe seguimiento documentado de los casos?



2do COLOQUIO DE CIBERSEGURIDAD



Escanear el QR

CONSULTA Y FUENTES

Protocolo provincial de Misiones (sitio oficial del Ministerio de Educación).

<https://edu.misiones.gob.ar/nuevo-protocoloprovincial-para-prevenir-y-actuar-ante-violencias-digitales-en-la-ninez-y-adolescencia/>

Leyes nacionales:

https://argentina.gob.ar/normativa_EDAYO

Revisar siempre la versión vigente del protocolo y los canales de derivación del SPEPM.

Documento orientativo: no reemplaza la normativa completa ni el asesoramiento especializado.

Ley Olimpia - Consulta rápida por QR



LEY OLIMPIA · TEXTO OFICIAL

Escanea el código QR para consultar la Ley 27.736 en el portal oficial de normativa argentina.

<https://www.argentina.gob.ar/normativa/nacional/ley-27736-391774/texto>

ISES