Guía de Actuación Institucional Rápida > PARA EL SISTEMA EDUCATIVO PROTOCOLO para la Prevención, Detección y Actuación ante RIESGOS Y VIOLENCIAS DIGITALES

Estructura y fases del protocolo + Triaje de riesgos
El presente protocolo establece un circuito de actuación institucional organizado en **cinco (5) fases sucesivas**, que orientan a las instituciones educativas en la prevención, detección, intervención, articulación y seguimiento de situaciones vinculadas a riesgos y violencias digitales, resguardando el interés superior de niñas, niños y adolescentes (NNyA) y delimitando claramente las responsabilidades educativas, administrativas y judiciales.

FASE 1 | DETECCIÓN Y PRIMERA ATENCIÓN

OBJETIVO Identificar tempranamente la situación, brindar contención inicial y activar el circuito institucional de protección.

ACCIONES

→ Detectar indicadores de riesgo a partir de:
- conductas del/la estudiante,
- interacciones digitales,
- comentarios, cambios emocionales,
- publicaciones, mensajes o señales de alerta.

→ Evaluar preliminarmente el nivel de riesgo conforme al Triaje Digital:
- Riesgo bajo: abordaje institucional interno.
- Riesgo medio o alto: activación de canales formales de actuación institucional y administrativo.

→ Establecer un primer contacto empático, escuchando sin juzgar, registrando el relato y el contexto sin exposición pública.
→ Explicar que no puede prometerse confidencialidad absoluta, aclarando que la información será compartida con los equipos responsables para garantizar la protección de derechos.
→ Dar aviso inmediato al Equipo Directivo y/o al Equipo de Orientación Escolar (EOE) / gabinete psicopedagógico.
→ Derivar a profesionales del equipo local para contención inicial (psicopedagogo/a, referente de Dirección de TIC | Huellas en la Red, o docente de referencia).

FASE 2 | REGISTRO, PRESERVACIÓN PRIMARIA Y PRIMERAS ACCIONES

OBJETIVO Documentar la situación, proteger la evidencia disponible y formalizar la actuación institucional.

ACCIONES

2.1 Registro institucional de los hechos
Documentar en actas institucionales los datos esenciales:
- Nombres de las personas involucradas,
- Fechas y contexto,
- Descripción objetiva de lo ocurrido,
- Evidencia disponible.

Utilizar los formatos establecidos en los Anexos (ficha de notificación, acta de intervención, ficha de seguimiento).

2.2 Preservación primaria no forense de evidencia digital
Resguardar mensajes, audios, imágenes o publicaciones relevantes, sin reenviarlos, editarlos ni difundirlos.
Registrar de manera precautoria:
- Fotografías o videos del contenido en el dispositivo contenedor,
- URLs, nombres de usuario, perfiles, números asociados. Evitar toda manipulación técnica del dispositivo, garantizando la integridad y confidencialidad de la información.

2.3 Articulación técnica con organismos especializados
Según la naturaleza, urgencia y características del hecho, la institución educativa podrá comunicarse de manera inmediata con organismos especializados para recibir orientación técnica (ver anexos-directorio):
- Fiscalía de Instrucción especializada en cibercrimen,
- Secretaría de Apoyo para Investigaciones Complejas (SAIC),
- Línea Contame,
- Cibercrimen de Jefatura o Unidades Regionales,
- Sistema de emergencias 911.

En hechos recientes (amenazas, grooming, intentos de extorsión), donde exista riesgo de pérdida de evidencia, se recomienda solicitar colaboración inmediata.
En hechos anteriores, se sugiere igual comunicación, adoptando medidas de preservación primaria no forense, sin intervención técnica.

2.4 Pautas de seguridad digital
Acompañar a la persona afectada y a su entorno en:
- Cambio de contraseñas,
- Revisión de configuraciones de privacidad,
- Resguardo de información sensible.

2.5 Circuito administrativo educativo
En casos de riesgo medio o alto, enviar correo institucional a la Dirección de TIC del Ministerio de Educación (protocoloDtic@gmail.com), quien gestionará el reenvío administrativo a:
- GPI (Gabinete Psicopedagógico Interdisciplinario),
- Dirección de Políticas Estudiantiles,
- Supervisión y Dirección de Nivel.

2.6 Responsabilidad de la denuncia judicial
La denuncia judicial corresponde a la familia o responsable legal, con orientación y acompañamiento de la institución.
Si la familia no pudiera o se negara, el Equipo Directivo, en articulación con Supervisión y Dirección de TIC, deberá dar aviso a la autoridad competente, dejando registro institucional.
La escuela no reemplaza la denuncia judicial, pero debe orientar, acompañar y documentar la actuación.

FASE 3 | EVALUACIÓN TÉCNICA Y DERIVACIÓN INTERINSTITUCIONAL

OBJETIVO Valorar la gravedad del caso y derivar según el nivel de riesgo.

ACCIONES

- Evaluar la situación de manera interdisciplinaria (EOE, Dirección, TIC, GPI).
- Determinar si se requiere intervención técnica especializada (seguridad digital, salud mental, asistencia legal).
  Según el riesgo:
    - Riesgo bajo: seguimiento institucional interno.
    - Riesgo medio: derivación educativa y contención psicológica.
    - Riesgo alto: derivación urgente a:
        - Esfera judicial: Fiscalía de Ciberdelitos o Fuerzas de Seguridad (911).
        - Esfera educativa: comunicación formal vía Dirección de TIC (protocoloDtic@gmail.com) quien remite a GPI, Políticas Estudiantiles y Supervisión.
- Garantizar contención emocional inmediata.
- Registrar todas las acciones en el cuaderno institucional y en el informe de derivación.

Cuando se utilicen herramientas de inteligencia artificial para análisis técnico (detección de alteraciones, contenidos sintéticos o deepfakes), su uso estará exclusivamente a cargo de organismos especializados (SAIC, OCEDIC, peritos, Dirección de TIC), sin sustituir el criterio profesional ni el proceso judicial, y respetando la cadena de custodia.

FASE 4 | INTERVENCIÓN Y ACOMPAÑAMIENTO

OBJETIVO Restituir derechos, reparar vínculos y asegurar la continuidad educativa.

ACCIONES

- Intervenir con enfoque pedagógico restaurativo, educativo y legal.
- Informar, contener y acompañar a la persona afectada y su familia.
- Involucrar al grupo o curso, cuando corresponda, mediante acciones de convivencia digital y empatía.
- Articular con organismos externos de salud, niñez, seguridad y justicia.
- En casos graves o reiterados, mantener comunicación con Dirección de TIC y GPI hasta el cierre administrativo.
- Aplicar medidas pedagógicas o restaurativas conforme al Reglamento Escolar.
- Garantizar la no revictimización.

FASE 5 | CIERRE Y EVALUACIÓN

OBJETIVO Consolidar aprendizajes institucionales y asegurar seguimiento.

ACCIONES

- Registrar todas las intervenciones realizadas, con fechas y responsables.
- Evaluar el impacto del acompañamiento:
    - ¿Se detuvo el daño digital?
    - ¿Se restituyó la convivencia?
    - ¿Hubo reincidencia?
- Reunir al equipo institucional (dirección, docentes, TIC, EOE) para analizar el caso y extraer aprendizajes.
- Actualizar el protocolo interno escolar si la experiencia lo amerita.
- Enviar informe final de cierre a la Dirección de TIC quien remite a GPI y Políticas Estudiantiles para registro centralizado. A su vez, a la Supervisión de Nivel.

OBSERVACIONES Y ACUERDOS ADMINISTRATIVOS

La vía administrativa institucional deberá activarse de manera obligatoria en todos los casos clasificados como riesgo medio o riesgo alto, conforme al triaje establecido en el presente Protocolo.
En este marco:
· Toda intervención deberá contar con respaldo legal y administrativo, articulándose con los organismos competentes del Consejo General de Educación y el Servicio Provincial de Enseñanza Privada de Misiones (SPEM), según corresponda.
· **La no activación del circuito administrativo, la omisión de actuaciones formales o el incumplimiento de los procedimientos previstos en el presente Protocolo podrán dar lugar a responsabilidades administrativas y eventualmente a la instrucción de sumario administrativo, de acuerdo con la normativa vigente.**
· Toda comunicación institucional vinculada a situaciones de riesgo o violencia digital deberá quedar registrada por escrito, utilizando actas, informes y correos electrónicos institucionales, conforme a los modelos anexos.
· **En los casos de riesgo alto, la omisión, dilación o negativa a realizar la denuncia correspondiente constituirá incumplimiento de los deberes funcionales, sin perjuicio de las responsabilidades que pudieran derivarse en otros ámbitos.**
· **Ningún docente ni directivo podrá intervenir de manera aislada. Toda actuación deberá ser documentada, elevada a las autoridades correspondientes y compartida con la red institucional, garantizando la adecuada articulación con las familias y los organismos intervinientes.**

Asimismo, el uso de herramientas digitales o de inteligencia artificial para el registro, análisis, almacenamiento o intercambio de información vinculada a situaciones de riesgo o violencia digital deberá respetar estrictamente la confidencialidad, la protección de datos personales y el principio de mínima exposición de la persona afectada, conforme a lo establecido por la Ley Nacional N.º 25.326 de Protección de Datos Personales y la normativa vigente.

En todos los casos, se priorizará el uso de sistemas institucionales seguros, evitando la utilización de cuentas personales, dispositivos no protegidos o plataformas no oficiales, y se garantizará que la información sea accesible únicamente a las autoridades y equipos competentes, preservando la intimidad y los derechos de niñas, niños y adolescentes.

TRIAJE PARA LA DETECCIÓN DE RIESGO EN SITUACIONES DE VIOLENCIA DIGITAL

RIESGO BAJO

ABORDAJE INSTITUCIONAL PREVENTIVO

Objetivo: fortalecer la prevención, el respeto digital y el acompañamiento cotidiano.
Características: situaciones leves o iniciales, sin exposición pública ni afectación emocional severa. Pueden resolverse dentro del ámbito escolar mediante estrategias pedagógicas, restaurativas y de alfabetización digital.
Indicadores:
- Comentarios o bromas en redes, sin intención directa de dañar.
- Discusiones entre pares en espacios digitales institucionales.
- Publicaciones o memes inapropiados, sin contenido violento.
- Participación pasiva en cadenas, grupos o desafíos sin riesgo.
- Cambios leves de comportamiento (aislamiento ocasional, irritabilidad).

ACCIONES SUGERIDAS

- Abordaje pedagógico dentro del aula o tutoría.
- Conversación privada con los involucrados para restaurar la convivencia.
- Registro en cuaderno institucional o acta de observación.
- **Intervención del EOE o equipo de convivencia escolar si lo hubiere.**
- Seguimiento por parte del docente y equipo directivo.
- **No requiere notificación administrativa ni judicial.**

RIESGO MEDIO

ABORDAJE INSTITUCIONAL Y VÍA ADMINISTRATIVA

Objetivo: activar la red institucional y garantizar acompañamiento integral.
Características: hechos que vulneran la intimidad, dignidad o bienestar de una persona, con repercusión en redes o grupos digitales, pero sin amenaza directa ni exposición masiva.
Pueden provocar angustia, aislamiento o conflicto sostenido.
Indicadores:
Reiteración de burlas o hostigamiento digital (ciberacoso leve o moderado).
- Difusión de mensajes o imágenes sin consentimiento.
- Suplantación de identidad, manipulación de fotos o edición de audios.
- Participación en desafíos virales de riesgo moderado.
- Expresiones de desesperanza o aislamiento emocional visible.

ACCIONES SUGERIDAS

- **Activar el Protocolo Institucional de Violencias Digitales.**
- **Informar a la Dirección de la Escuela y al EOE.**
- **Comunicar la situación al Supervisor/a de Nivel.**
- **Elaborar acta institucional con firmas de los intervinientes.**
- **Enviar correo oficial a la Dirección de TIC del Ministerio de Educación (protocoloDtic@gmail.-com), para que ésta realice el reenvío administrativo a:**
  · GPI (Gabinete Psicopedagógico Interdisciplinario)
  · Dirección de Políticas Estudiantiles
  · Supervisores y Direcciones de Nivel
- **Contactar a la familia o adulto responsable, garantizando la contención.**
- Denunciar contenido dañino en la plataforma correspondiente.
- **En los casos en que se identifiquen indicadores de autolesión, sufrimiento psíquico o posible riesgo suicida, la institución educativa deberá activar de manera inmediata la articulación con el sistema de salud, garantizando el acceso a una respuesta profesional especializada.**

En este marco, se dispone la derivación al Equipo de Salud Mental Provincial, dependiente de la Dirección de **Salud Mental del Ministerio de Salud Pública**, asegurando una intervención oportuna, integral y basada en evidencia.

A tales fines, el Ministerio de Salud pone a disposición un ecosistema de salud digital que permite una atención accesible, continua y territorialmente equitativa, integrado por los siguientes dispositivos:
Asistente Virtual "Chavy": herramienta de atención inmediata que posibilita una primera escucha virtual a cargo de profesionales del equipo de salud mental, la evaluación inicial del riesgo y, en caso de ser necesario, la derivación a una consulta presencial en el efector de salud más cercano al domicilio de la persona, conforme al nivel de complejidad requerido.
Plataforma Alegra Med: sistema de gestión de turnos programados para atención virtual en salud mental, que permite la autogestión de consultas con profesionales especializados, garantizando el acceso remoto desde cualquier punto de la provincia, la disponibilidad de historia clínica electrónica unificada y la emisión de recetas o certificados digitales, optimizando los tiempos de respuesta y evitando traslados innecesarios.
El abordaje sanitario se encuentra alineado con el marco normativo vigente, los criterios diagnósticos del DSM-5 y la Guía de Intervención mhGAP (Mental Health Gap Action Programme) de la OMS/OPS, asegurando prácticas basadas en evidencia y una cobertura equitativa en el acceso a la atención en salud mental.
Asimismo, la articulación con el Ministerio de Salud Pública se inscribe en una estrategia de trabajo intersectorial que reconoce a las violencias digitales como una problemática compleja, con impacto directo en el bienestar psicofísico de niñas, niños y adolescentes, y que requiere respuestas coordinadas entre el sistema educativo y sanitario.
Finalmente, ante situaciones que lo requieran, podrá gestionarse la derivación a otros dispositivos de la Red Asistencial Provincial de Complejidad Ascendente, garantizando la continuidad del cuidado desde el primer nivel de atención hasta los niveles de mayor complejidad.
- **En caso de negativa de atención, notificar a la Defensoría de los Derechos de Niños, Niñas y Adolescentes.**

RIESGO ALTO

INTERVENCIÓN URGENTE Y ARTICULACIÓN JUDICIAL

Objetivo: proteger la vida, detener el daño y activar de inmediato las redes de salud, justicia y educación.
Características: situaciones de grave vulneración de derechos, violencia psicológica o sexual digital, exposición masiva, amenazas, coacción o peligro inminente para la integridad emocional o física.
Incluye delitos informáticos y autolesiones vinculadas al entorno digital.
Indicadores:
- Grooming, sextorsión, amenazas o chantajes en línea.
- Visualización de material íntimo o humillante.
- Hostigamiento sostenido con fines de control o persecución.
- Publicaciones que inciten al suicidio o al cutting.

ACCIONES SUGERIDAS

- **El docente o directivo debe efectuar la denuncia inmediata ante la autoridad institucional.**
- **Activar simultáneamente:**
  · Vía administrativa: correo urgente a la Dirección de TIC (protocoloDtic@gmail.com), que reenviará a GPI, Políticas Estudiantiles, Supervisión y Dirección de Nivel.
  · Vía judicial (independiente de la educativa): orientar y acompañar a la familia o docentes para denunciar en Fiscalía de Ciberdelitos, Policía o Línea 911.
- Preservar evidencias digitales sin compartirlas.
- No dejar sola a la persona afectada; garantizar contención inmediata.
- Registrar todas las actuaciones en actas institucionales.
- **Si el hecho involucra a un/a docente como víctima, activar el GPI y si involucra a un estudiante al área de Política Estudiantil.**

En todos los casos en que se identifiquen indicadores de autolesión, riesgo suicida o afectación severa de la salud mental, se deberá activar de manera inmediata la articulación con el sistema de salud, garantizando una respuesta profesional urgente.
A tal efecto, se dispone la intervención del Equipo de Salud Mental Provincial, dependiente de la Dirección de **Salud Mental del Ministerio de Salud Pública**, asegurando una atención integral, continua y basada en evidencia.
El Ministerio de Salud pone a disposición un ecosistema de salud digital, que permite una respuesta inmediata y territorialmente accesible, integrado por:
Asistente Virtual "Chavy": dispositivo de primera escucha inmediata, que posibilita la evaluación inicial del riesgo por parte de profesionales de salud mental y, de ser necesario, la derivación urgente a un efector de salud cercano al domicilio, conforme al nivel de complejidad requerido.
Plataforma Alegra Med: sistema de gestión de turnos para atención virtual en salud mental, que permite el acceso remoto a profesionales especializados, la continuidad del seguimiento, la disponibilidad de historia clínica electrónica unificada y la emisión de recetas o certificados digitales.
Este abordaje se encuentra alineado con el marco normativo vigente, los criterios del DSM-5 y la Guía de Intervención mhGAP (OMS/OPS), garantizando prácticas basadas en evidencia, intervención oportuna y cobertura equitativa en salud mental.
Asimismo, la articulación con el sistema sanitario se integra a la Red Asistencial Provincial de Complejidad Ascendente, asegurando la continuidad del cuidado desde el primer nivel de atención hasta los niveles de mayor complejidad.