Política de Seguridad Online

Aprobado por: Raúl Fernández Pascual, Director del Colegio CEDES	**Última revisión:** Junio 2026
Próxima revisión: Junio 2027	

1. Propósito

La seguridad online constituye una parte integral de la salvaguarda y protección del alumnado (safeguarding), y contribuye a proteger a la comunidad educativa frente a riesgos como la exposición a contenidos perjudiciales, el ciberacoso, el grooming y la radicalización.

Esta política tiene como finalidad garantizar que el alumnado pueda beneficiarse de las oportunidades que ofrece Internet de forma segura, minimizando los posibles riesgos y daños.

2. Ámbito de aplicación

Esta política se aplica a todos los miembros de la comunidad educativa —personal, alumnado, padres/madres/tutores legales, visitantes, voluntarios y otros usuarios de la comunidad— que utilicen los sistemas, dispositivos, recursos tecnológicos y redes digitales del centro, tanto dentro como fuera del mismo.

Cuando el centro escolarice o derive temporalmente a un alumno a un proveedor educativo alternativo, continuará siendo responsable de su salvaguarda y protección. Se realizará con dicho proveedor una evaluación conforme a esta política y el centro deberá obtener confirmación por escrito de que existen medidas adecuadas de seguridad online.

3. Legislación y marco de referencia

La guía estatutaria Keeping Children Safe in Education (KCSIE) establece definiciones y orientaciones sobre los riesgos online, incluidos aquellos relacionados con la Inteligencia Artificial (IA) y las tecnologías deepfake. La legislación española relevante incluye la Ley Orgánica 8/2021, de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI); la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD); el Reglamento (UE) 2016/679, General de Protección de Datos (RGPD); y la Ley Orgánica 2/2006, de Educación (LOE), modificada por la Ley Orgánica 3/2020 (LOMLOE).

De acuerdo con la Education and Inspections Act 2006 del Reino Unido, los directores (Principals) disponen de facultades para intervenir ante determinadas conductas del alumnado producidas fuera del centro, y el personal puede aplicar medidas disciplinarias ante conductas inapropiadas vinculadas a la pertenencia al centro, incluido el ciberacoso. La Education Act 2011 (Section 24b) amplía estas facultades para incluir la revisión de dispositivos electrónicos y la eliminación de datos.

En España, el marco correspondiente viene establecido por la Ley Orgánica 2/2006, de Educación (LOE), modificada por la Ley Orgánica 3/2020 (LOMLOE); la Ley Orgánica 8/2021 (LOPIVI); así como por la normativa educativa autonómica aplicable y los procedimientos del centro relativos a la conducta del alumnado, safeguarding, seguridad online y uso de dispositivos electrónicos personales.

El centro abordará las conductas inapropiadas en el entorno online mediante las políticas y procedimientos correspondientes e informará a los padres/madres/tutores legales cuando se detecten comportamientos online inadecuados fuera del centro que requieran intervención.

3.1 Tipos de riesgos

El conjunto de riesgos incluidos dentro de la **seguridad online** es amplio y está en constante evolución, pero puede clasificarse en cuatro grandes áreas:

- **Contenido (Content):** exposición a contenidos ilegales, inapropiados o perjudiciales, incluidas imágenes, audios o vídeos generados mediante **Inteligencia Artificial (IA)**.

Algunos ejemplos son la pornografía, el racismo, la misoginia, las autolesiones, el suicidio, el antisemitismo, la radicalización, el extremismo, la suplantación de identidad, la información errónea, la desinformación —incluidas las noticias falsas (fake news)— y las teorías de la conspiración.

- **Contacto (Contact):** exposición a interacciones online perjudiciales con otros usuarios.

Algunos ejemplos son la presión entre iguales, la publicidad comercial o el contacto con adultos que se hacen pasar por niños, adolescentes o jóvenes con la intención de realizar **grooming** o explotarlos con fines sexuales, delictivos, económicos o de cualquier otra naturaleza.

- **Conducta (Conduct):** comportamientos online que aumentan la probabilidad de causar un daño o que lo provocan directamente.

Algunos ejemplos son la creación, envío, recepción o difusión de imágenes explícitas —incluido el intercambio, consentido o no consentido, de imágenes de desnudos o semidesnudos y/o pornografía—, el acoso y el **ciberacoso**.

- **Comercio (Commerce):** riesgos relacionados con actividades comerciales o económicas online, como los juegos de azar, la publicidad inapropiada, el phishing o las estafas económicas.

3.2 Contenido inapropiado

Se espera que:

- Se impida de forma eficaz y fiable que los usuarios generen o accedan a contenidos perjudiciales o inapropiados.
- Los estándares y sistemas de filtrado se mantengan de forma efectiva durante toda la duración de una conversación o interacción con un usuario.
- El filtrado se adapte en función de los diferentes niveles de riesgo, edad, adecuación del contenido y necesidades del usuario, incluyendo, por ejemplo, al alumnado con necesidades educativas especiales y discapacidad (SEND).
- El contenido multimodal sea moderado eficazmente, incluyendo la detección y el filtrado de contenidos prohibidos en diferentes idiomas, imágenes, errores ortográficos habituales y abreviaturas.
- Se mantenga una capacidad completa de moderación de contenidos, independientemente del dispositivo utilizado, incluidos los dispositivos personales (Bring Your Own Device – BYOD) y los teléfonos móviles cuando se acceda a productos o servicios mediante una cuenta institucional educativa.
- Los contenidos sean moderados teniendo en cuenta adecuadamente el contexto de la conversación o interacción, garantizando que cualquier contenido generado sea sensible y apropiado al contexto.
- Los sistemas de filtrado se actualicen periódicamente para responder a nuevos riesgos o tipos emergentes de contenido perjudicial, así como a las nuevas herramientas de Inteligencia Artificial (IA) a las que puedan acceder los usuarios.

4. Roles y responsabilidades

Todas las personas, incluidos los **visitantes externos**, profesores de prácticas, monitores deberán leer y aceptar la **Política de Uso Aceptable de las Tecnologías de la Información (Acceptable Use of IT Policy)** antes de acceder y utilizar los sistemas y redes locales y online del centro.

Las siguientes responsabilidades en materia de **seguridad online** corresponden a los distintos roles:

4.1 Órgano de gobierno (school board)

- Aprobar la **Política de Seguridad Online**.

- Revisar la eficacia de la política teniendo en cuenta la información y valoración proporcionadas por el **Regional Head of Schools (RHoS)**.

4.2 Regional head of schools (RHOS)

- Actuar como miembro del **Operational Board** responsable de la Seguridad Online, lo que incluye:
  - Mantener reuniones periódicas con el **Coordinador/a de Seguridad Online / Coordinadora de Bienestar y Protección (DSL) / Director (Principal)**.
  - Revisar y aprobar cualquier modificación de la política.
  - Supervisar los incidentes y registros relacionados con la seguridad online.
  - Informar de los incidentes al **Operational Board**.

4.3 Director (principal) y equipo directivo

- Garantizar la **seguridad de la comunidad educativa**.
- Garantizar que exista una autoridad o capacidad de actuación equivalente conforme a la **legislación local aplicable**.
- Garantizar la existencia de un sistema para la **supervisión, comunicación y recepción de informes de incidentes** por parte del Responsable de Seguridad Online / **Designated Safeguarding Lead (DSL)**.
- Delegar las responsabilidades cotidianas relativas a la seguridad online en el Responsable de Seguridad Online / **Designated Safeguarding Lead (DSL)**.
- Garantizar que todo el personal reciba una **formación adecuada**.

4.4 Responsable de seguridad online / coordinadora de bienestar y protección (DSL) o deputy DSL

- Liderar el **Grupo de Seguridad Online**.
- Gestionar los incidentes cotidianos relacionados con la seguridad online y mantener un **registro de todos los incidentes**.
- Revisar los procedimientos y la política, y comunicar al equipo directivo posibles mejoras o situaciones de incumplimiento.
- Proporcionar **formación y asesoramiento** a todo el personal.
- Coordinarse con el personal técnico y con las **autoridades u organismos externos competentes**.

4.5 Responsable de redes/it y personal técnico

- Mantenerse actualizado respecto a las políticas, procedimientos, buenas prácticas y formación en materia de seguridad online.
- Garantizar la seguridad física de la infraestructura tecnológica del centro.
- Implementar y supervisar las medidas de seguridad online y garantizar que se mantengan actualizadas, incluidas la protección mediante firewall y antivirus.
- Garantizar que toda la tecnología relacionada con el acceso online esté protegida de acuerdo con la normativa local, la Política de Seguridad Online y los estándares establecidos por el grupo.
- Garantizar que cualquier proveedor externo contratado cumpla las medidas de seguridad online y conozca plenamente los procedimientos del centro antes de comenzar a trabajar en él.
- Garantizar que las plataformas de mensajería y colaboración sean supervisadas para detectar posibles usos indebidos y, en caso de incidente, comunicarlo al Responsable de Seguridad Online y al equipo directivo para su investigación.
- Garantizar que el acceso físico a los sistemas informáticos esté restringido al nivel adecuado y que los usuarios dispongan de permisos de acceso claramente definidos. Esto incluye el almacenamiento online y extraíble, los sistemas de datos del personal y del alumnado, los datos de la organización y el acceso a Internet.
- Garantizar que todo el alumnado y el personal dispongan de un nombre de usuario y una contraseña que cumplan los estándares de seguridad establecidos en la Política de Contraseñas (Password Policy), y que no se utilicen cuentas genéricas en los sistemas del centro.

- Garantizar que todos los nombres de usuario y contraseñas de administración principal se almacenen en una bóveda cifrada, y que el Director tenga acceso a ella en caso de emergencia para garantizar la continuidad operativa.
- Garantizar que todas las licencias de software estén actualizadas y cubran el número de usuarios y dispositivos utilizados en el centro.
- Garantizar que todo acceso a Internet disponga de un filtrado adecuado a la edad y al rol del usuario, que el firewall y las pasarelas de seguridad estén actualizados y que los controles de seguridad reflejen las medidas de salvaguarda establecidas en la Safeguarding Controls Policy.
- Apoyar al Responsable de Seguridad Online / DSL para garantizar la existencia de un sistema que permita supervisar, registrar y comunicar los incidentes de seguridad online.
- Garantizar que la Política de Uso Aceptable de las Tecnologías de la Información esté disponible para el personal, el alumnado, las familias y los colaboradores externos, y que se aplique antes de conceder acceso a los sistemas y redes del centro.
- Realizar una evaluación anual de riesgos de ciberseguridad y revisarla cada trimestre.
- Desarrollar e implementar un plan de copias de seguridad de los datos del centro y revisarlo anualmente.
- Comunicar todos los ciberataques.

4.6 Personal docente y de apoyo

- Leer, comprender y cumplir la Política de Seguridad Online y la Política de Uso Aceptable de las Tecnologías de la Información.
- Mantenerse actualizado en materia de seguridad online.
- Integrar la seguridad online en el currículo.
- Supervisar y orientar al alumnado en el uso de las tecnologías digitales.
- Comunicar cualquier uso indebido al Responsable de Seguridad Online y al equipo directivo para su investigación.
- Garantizar que todas las comunicaciones con el alumnado y las familias se realicen mediante los sistemas oficiales del centro y que tengan siempre un carácter profesional.
- Garantizar que el alumnado comprenda la Política de Seguridad Online y sepa cómo evitar el plagio y las vulneraciones de los derechos de autor.
- En las clases en las que se haya planificado previamente el uso de Internet, orientar al alumnado hacia sitios web cuya idoneidad haya sido comprobada y garantizar que existan procedimientos para actuar ante cualquier contenido inapropiado que pueda aparecer durante las búsquedas.
- Supervisar y aplicar las políticas vigentes relativas al uso de dispositivos cuando se permita utilizar tecnologías digitales, dispositivos móviles, cámaras u otros equipos durante las clases y demás actividades escolares.

4.7 Alumnado

- Conocer y comprender la Política de Seguridad Online y la Política de Uso Aceptable de las Tecnologías de la Información.
- Utilizar responsablemente los sistemas y recursos tecnológicos del centro, de acuerdo con la Política de Uso Aceptable de las Tecnologías de la Información.
- Comunicar cualquier uso indebido o contenido inapropiado.
- Seguir las orientaciones de buenas prácticas relativas, entre otras cuestiones, a la toma y uso seguro de imágenes y al uso adecuado de teléfonos móviles, y desarrollar una adecuada comprensión del ciberacoso.

4.8 Padres, madres y tutores legales

- Apoyar las políticas del centro en materia de seguridad online.
- Supervisar la actividad online de sus hijos.
- Comprender la importancia de una adecuada seguridad online y las prácticas que esta implica, prestando especial atención a:
  - El uso seguro y responsable de los dispositivos personales.
  - La toma y utilización de fotografías y vídeos digitales durante las actividades y eventos del centro y en su entorno.

- Las orientaciones sobre acceso y uso compartido seguro de la información en las secciones destinadas a las familias de las plataformas educativas y en los registros online del alumnado.

5. Educación y formación

Aunque la regulación y las medidas técnicas son importantes, es fundamental educar al alumnado para que actúe de forma segura y responsable en el entorno online. La seguridad online y la competencia digital son elementos esenciales de la formación que ofrece el centro, ayudando al alumnado a identificar riesgos y desarrollar estrategias de protección y resiliencia.

La seguridad online deberá integrarse de forma transversal en el currículo, y el personal reforzará de manera continuada los mensajes clave. El currículo de seguridad online deberá ser amplio, adecuado a la edad y permitir una progresión en el aprendizaje mediante propuestas educativas diversas y creativas, adaptadas a la estructura del centro y a las diferentes edades del alumnado.

5.1 Educación del alumnado

Para garantizar un enfoque coherente y eficaz de la seguridad online, el centro adoptará las siguientes medidas:

- **Desarrollo curricular:** se impartirá un programa estructurado de seguridad online a través de **Tecnología y Digitalización, Educación en Valores y otras materias o áreas pertinentes**, reforzando periódicamente sus contenidos.
- **Mensajes para toda la comunidad escolar:** los principales mensajes sobre seguridad online se incorporarán a las asambleas, tutorías y programas de acción tutorial y bienestar.
- **Pensamiento crítico:** se enseñará al alumnado a **evaluar críticamente los contenidos online** y comprobar la fiabilidad y veracidad de la información.
- **Responsabilidad digital:** se incluirán orientaciones sobre la correcta identificación y citación de las fuentes y el respeto a los **derechos de autor y la propiedad intelectual**.
- **Resiliencia frente a la radicalización:** se ayudará al alumnado a desarrollar herramientas de protección frente a la radicalización mediante el debate seguro sobre temas controvertidos y la comprensión de la **participación cívica y democrática frente al extremismo**.
- **Uso aceptable:** se educará al alumnado sobre la importancia de la **Política de Uso Aceptable de las Tecnologías de la Información (Acceptable Use of IT Policy)** y se fomentará un uso responsable de la tecnología tanto dentro como fuera del centro.
- **Personal como modelo de conducta:** el personal deberá actuar como modelo de **uso adecuado, seguro y responsable** de las tecnologías digitales, Internet y los dispositivos móviles.
- **Prácticas de navegación segura:** cuando el uso de Internet haya sido planificado previamente, se dirigirá al alumnado a sitios web cuya idoneidad haya sido comprobada y existirán procedimientos para actuar ante la posible aparición de contenidos inapropiados.
- **Supervisión:** cuando el alumnado disponga de acceso abierto a Internet, el personal **supervisará activamente su actividad**.
- **Acceso a contenidos restringidos:** cuando exista una finalidad educativa legítima —por ejemplo, investigaciones relacionadas con racismo, drogas o discriminación—, el personal podrá solicitar acceso temporal a sitios web bloqueados. Estas solicitudes deberán quedar **registradas, ser justificadas y permitir su posterior revisión**, y podrán ser autorizadas por el Director (Principal), en consulta con el **Regional Head of Schools (RHoS)** cuando sea necesario.

5.2 Formación e implicación de las familias

Las familias desempeñan un papel fundamental en la orientación y supervisión de la actividad online de sus hijos. Sin embargo, algunas pueden desconocer los riesgos existentes o cómo actuar ante una preocupación relacionada con la seguridad online.

Para apoyar a las familias, el centro promoverá la sensibilización y proporcionará información periódica a través de:

- Actividades relacionadas con el currículo.
- Comunicaciones del centro, como cartas, boletines informativos, página web o plataforma educativa.
- Sesiones informativas, talleres y actividades dirigidas a las familias.
- Campañas de sensibilización, como el **Día de Internet Segura (Safer Internet Day)**.
- Orientación hacia **recursos fiables y especializados**.
- Información y recursos que ayuden a las familias a fomentar la seguridad online en el hogar.

5.3 Formación e implicación del personal y voluntariado

- Todo el personal recibirá periódicamente formación formal y registrada en seguridad online, como parte de su plan de Desarrollo Profesional Continuo (CPD) y de la formación obligatoria.
- El personal de nueva incorporación recibirá formación en seguridad online como parte de su proceso de acogida e incorporación (induction), que deberá completarse durante las tres primeras semanas.
- Todo el personal revisará y aceptará formalmente la Política de Seguridad Online y las demás políticas relacionadas al comienzo de cada curso escolar o, en el caso de nuevas incorporaciones durante el curso, como parte de su proceso de induction.

5.4 Regional head of schools (RHOS) y órgano de gobierno (school board)

- Participarán periódicamente en **formación formal y registrada sobre seguridad online**, como parte de su plan de Desarrollo Profesional Continuo (CPD) y de formación obligatoria.

6. Actuación ante incidentes de uso indebido

Este apartado establece las actuaciones que deben seguirse ante incidentes relacionados con el uso indebido de las tecnologías y tiene como finalidad garantizar que:

- Se sigan procedimientos claros para la gestión de los incidentes.
- Los incidentes graves sean comunicados inmediatamente a las autoridades u organismos competentes, cuando corresponda.

6.1 Incidentes

Durante la investigación de un incidente, el equipo directivo deberá:

- Involucrar al menos a dos miembros del equipo directivo, garantizando así la responsabilidad y supervisión del proceso.
- Utilizar un ordenador específicamente designado, al que el alumnado no tenga acceso. Este dispositivo podría ser requerido posteriormente por la Policía.
- Garantizar que las personas encargadas de la investigación dispongan de un acceso a Internet supervisado y registrado.
- Mantener una cronología de los hechos ante la posibilidad de que sea necesario informar posteriormente a la Policía.
- Registrar las URL y describir los contenidos que generan preocupación. La realización y conservación de capturas de pantalla puede resultar útil, pero nunca deberán realizarse ni almacenarse capturas que contengan imágenes de abuso sexual infantil.

Una vez realizada la investigación, el equipo directivo determinará si la preocupación está fundamentada y adoptará las medidas correspondientes, que podrán incluir:

- Medidas disciplinarias internas.
- Derivación o comunicación al Regional Head of Schools (RHoS) y/o a otros organismos o autoridades competentes.
- Intervención de la Policía, cuando corresponda.

6.2 Comunicación obligatoria a la policía

Determinados incidentes deberán ser comunicados a la Policía:

- **Imágenes de abuso sexual infantil.**
- Conductas de **grooming**.
- Envío de material obsceno o sexualmente inapropiado a un menor.
- Infracciones relacionadas con la publicación o difusión de material obsceno.
- Contenidos racistas que puedan constituir un **delito**.
- Promoción del **terrorismo o el extremismo**.
- Otras actividades que puedan constituir un **delito**.

6.3 Medidas de salvaguarda

- El ordenador utilizado para la investigación deberá mantenerse aislado, con el fin de preservar las evidencias y evitar cualquier posibilidad de manipulación.
- Todas las actuaciones realizadas deberán registrarse en un registro cronológico, creando así una trazabilidad clara de las evidencias a efectos de salvaguarda y posibles actuaciones legales.
- El formulario o registro de investigación, una vez completado, deberá conservarse como documentación de referencia.

6.4 Actuaciones y medidas disciplinarias

Es importante que cualquier incidente sea gestionado **lo antes posible y de manera proporcionada**. Asimismo, es importante que los miembros de la comunidad educativa tengan constancia de que los incidentes han sido debidamente gestionados.

En los **Anexos** se incluye un diagrama de flujo del procedimiento, así como propuestas de actuaciones y medidas disciplinarias aplicables ante distintos tipos de incidentes.

7. Seguimiento y revisión

Esta política ha sido elaborada por un grupo de trabajo compuesto por:

- Director (Principal) / Equipo Directivo.
- Responsable de Seguridad Online / **Coordinadora de Bienestar y Protección (Designated Safeguarding Lead – DSL)**.
- Personal del centro (personal docente, de apoyo y técnico).
- **Regional Head of Schools (RHoS) / Board**.
- Familias.
- Representantes del alumnado.

7.1 Calendario de seguimiento, revisión y desarrollo

- **Aprobación V1:** por el Board, el 31/07/2025.
- **Seguimiento:** por el Equipo Directivo, al menos una vez al año.
- **Informes:** anualmente al **Regional Head of Schools (RHoS)** y al Board, con **comunicación inmediata en caso de incidentes graves**.
- **Revisión:** anualmente, o cuando sea necesario debido a nuevos desarrollos o tras producirse incidentes, por el **RHoS en representación del Board**.

8. Políticas y documentos relacionados

Esta política deberá leerse conjuntamente con los siguientes documentos:

- Política de Salvaguarda y Protección Infantil (Safeguarding Policy).
- Política de Conducta (Behaviour Policy) y Política contra el Acoso Escolar (Anti-Bullying Policy).

- Política de Uso Aceptable de las Tecnologías de la Información (Acceptable Use of IT Policy), Política de Inteligencia Artificial (AI Policy), Política de Contraseñas (Password Policy), Política de Redes Sociales (Social Media Policy) y Política de Controles de Salvaguarda (Safeguarding Controls Policy).
- Keeping Children Safe in Education (KCSIE) 2026.

9. Recursos españoles

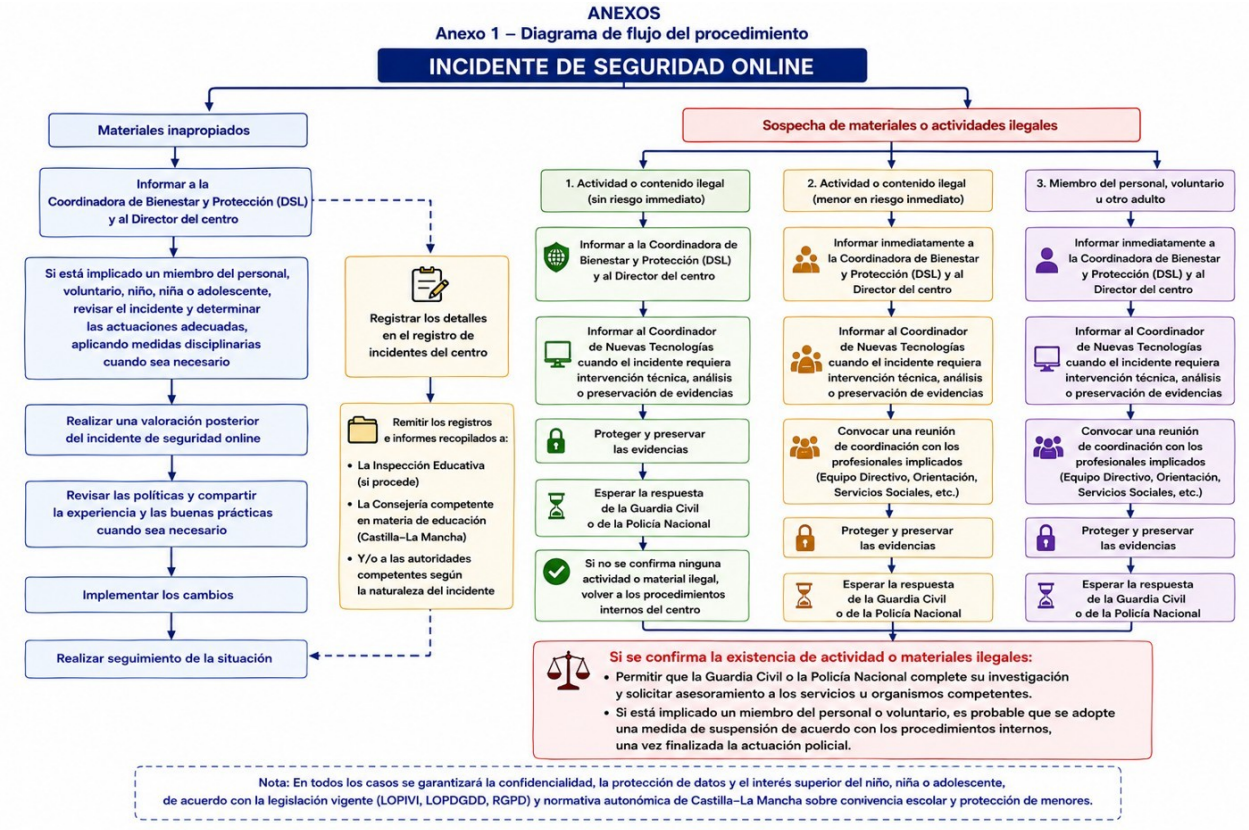
- **INCIBE – Instituto Nacional de Ciberseguridad / Internet Segura for Kids (IS4K):** Centro de Seguridad en Internet para menores en España, que proporciona recursos dirigidos al alumnado, las familias y los profesionales de la educación sobre **ciberacoso, grooming, sexting, contenidos perjudiciales, privacidad y uso seguro de la tecnología**.
  Internet Segura for Kids (IS4K)
- **INCIBE – Línea de Ayuda en Ciberseguridad 017:** servicio nacional, gratuito y confidencial, que ofrece asesoramiento sobre **ciberseguridad y seguridad online**, incluyendo ciberacoso, grooming, sexting, contenidos perjudiciales y otros riesgos online que puedan afectar a niños, niñas y adolescentes.
  Línea de Ayuda en Ciberseguridad 017
- **Agencia Española de Protección de Datos (AEPD) – Menores y Educación:** orientaciones sobre **privacidad de los menores, protección de datos personales, derechos digitales y uso de la tecnología en el ámbito educativo**.
  AEPD – Menores y Educación
- **AEPD – Canal Prioritario:** mecanismo que permite solicitar la **retirada urgente de contenidos sexuales o violentos difundidos en Internet sin consentimiento**, especialmente cuando puedan suponer un grave riesgo para los derechos y el bienestar de la persona afectada.
  AEPD – Canal Prioritario
- **INTEF – AseguraTIC:** recursos educativos sobre **seguridad online de los menores** dirigidos a centros educativos, profesorado, familias y alumnado, con materiales sobre ciberacoso, sexting, identidad digital, privacidad y uso seguro de la tecnología.
  INTEF – AseguraTIC
- **Ministerio de Educación, Formación Profesional y Deportes – Orientaciones sobre acoso y ciberacoso:** marco de referencia para la **prevención, detección e intervención ante situaciones de acoso escolar y ciberacoso** en los centros educativos.
  Ministerio de Educación – Acoso y ciberacoso

Recursos en Castilla-La Mancha

- **Consejería de Educación de Castilla-La Mancha – Protocolo de Acoso Escolar:** orientaciones y procedimientos autonómicos para la **prevención, identificación e intervención ante situaciones de acoso escolar**, incluidas aquellas relacionadas con las redes sociales y los entornos digitales.
  Castilla-La Mancha – Acoso escolar
- **Castilla-La Mancha – Marco normativo de Convivencia Escolar:** normativa y orientaciones autonómicas sobre **convivencia escolar, derechos y deberes del alumnado, protección y bienestar, y prevención e intervención ante situaciones de acoso**.
  Castilla-La Mancha – Convivencia Escolar
- **Programa #TúCuentas:** programa de Castilla-La Mancha dirigido a la **prevención, detección temprana e intervención profesional ante situaciones de acoso y ciberacoso** que afecten a niños, niñas y adolescentes.
  Castilla-La Mancha – Acoso escolar y Programa #TúCuentas

Anexos

Anexo 1 – Diagrama del proceso



Anexo 2 – Incidentes relacionados con el alumnado y actuaciones

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
Descarga o carga no autorizada de archivos	Advertencia	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Reiteración de las infracciones anteriores, tras advertencias o sanciones previas	Sanción adicional, p. ej., permanencia en el centro fuera del horario / expulsión	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Acceso accidental a material ofensivo o pornográfico y no comunicación del incidente	Advertencia	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Acceso deliberado o intento de acceso a material ofensivo o pornográfico	Suspensión	Retirada derecho de acceso a internet	Derivar al Director	Informar a familia	Derivar a la Policía

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
Acceso deliberado o intento de acceso a material que pueda considerarse ilegal	Suspensión	Retirada derecho de acceso a internet	Derivar al Director	Informar a familia	Derivar a la Policía
Uso de sitios proxy u otros medios para eludir el sistema de filtrado del centro	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Actuaciones que puedan desacreditar al centro o vulnerar la integridad y los principios éticos del mismo	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Incumplimiento de los derechos de autor o de las normas sobre licencias	Advertencia	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Alteración o destrucción de los datos de otros usuarios	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al Director	Informar a familia	Derivar a la Policía
Uso negligente de datos personales, p. ej., almacenamiento o transferencia de datos de forma no segura	Advertencia	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Permitir que otras personas accedan a la red del centro compartiendo el nombre de usuario y las contraseñas, o intentar acceder o acceder a la red del centro utilizando la cuenta de otra persona	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Actuaciones deliberadas destinadas a vulnerar las	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al Director	Informar a familia	Derivar a la Policía

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
normas de protección de datos o de seguridad de la red					
Uso personal inapropiado de Internet / redes sociales / correo electrónico personal	Advertencia	Retirada derecho de acceso a internet	Derivar al tutor	Informar a familia	–
Envío de un correo electrónico, mensaje de texto o mensaje que se considere ofensivo, constitutivo de acoso o de naturaleza intimidatoria	Medida disciplinaria	Retirada derecho de acceso a internet	Derivar al Director	Informar a familia	Derivar a la Policía

Anexo 3 – Incidentes relacionados con el personal y actuaciones

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
Actuaciones que puedan comprometer la conducta, integridad o reputación profesional de un miembro del personal	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Descarga o carga no autorizada de archivos	Advertencia	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS
Reiteración de las conductas anteriores tras advertencias o sanciones previas	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Acceso accidental a material ofensivo o pornográfico y no comunicación del incidente	Advertencia	Medida disciplinaria	Informar al Director	Informar al RHoS	—
Acceso deliberado o intento de acceso a material	Suspensión	Informar al Director	Informar al RHoS	Informar a la Policía	—

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
ofensivo o pornográfico					
Acceso deliberado o intento de acceso a material que pueda considerarse ilegal	Suspensión	Informar al Director	Informar al RHoS	Informar a la Policía	—
Uso de sitios proxy u otros medios para eludir el sistema de filtrado del centro	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Actuaciones que puedan desacreditar al centro o vulnerar sus principios y valores	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Incumplimiento de los derechos de autor o de las condiciones de las licencias	Advertencia	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS
Alteración o destrucción de los datos de otros usuarios, o daños deliberados al hardware o software	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	Informar a la Policía
Uso negligente de datos personales, por ejemplo, su almacenamiento o transferencia de forma no segura	Advertencia	Medida disciplinaria	Informar al Director	Informar al RHoS	—
Permitir a otras personas acceder a la red del centro compartiendo nombres de usuario y contraseñas, o intentar acceder o acceder a la red utilizando la cuenta de otra persona	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Actuaciones deliberadas	Medida	Suspensión	Informar al	Informar al RHoS	Informar a la

Escenario	Actuación 1	Actuación 2	Actuación 3	Actuación 4	Actuación 5
destinadas a vulnerar las normas de protección de datos o de seguridad de la red	disciplinaria		Director		Policía
Uso personal inapropiado de Internet, redes sociales o correo electrónico personal	Advertencia	Medida disciplinaria	Informar al Director	Informar al RHoS	—
Uso del correo electrónico personal, redes sociales, mensajería instantánea o mensajes de texto para mantener comunicaciones digitales con el alumnado	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	—
Envío de correos electrónicos, mensajes de texto u otros mensajes de carácter ofensivo, constitutivos de acoso o intimidación	Medida disciplinaria	Suspensión	Informar al Director	Informar al RHoS	Informar a la Policía