

Módulo 4. Ciber escudos y secretos digitales

Módulo 4. Ciber escudos y secretos digitales



Imagen generada con IA (Midjourney) (CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En el módulo '**Ciber escudos y secretos digitales**', elevamos nuestra preparación en ciberseguridad al siguiente nivel, enfocándonos en la creación de barreras robustas que protejan nuestro entorno educativo digital. Este módulo no solo te enseñará sobre la importancia de cumplir con la **Ley Orgánica de Protección de Datos (LOPD)** en las aulas, sino que también te dotará de las herramientas necesarias para salvaguardar a los menores en línea.

Explorarás métodos para fomentar una cultura de seguridad digital entre tus estudiantes, aprendiendo a manejar y responder a los retos que plantea el **ciberbullying**, y descubrirás cómo desarrollar **resiliencia digital**, capacitándote para anticipar y reaccionar ante incidentes cibernéticos.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>

Módulo 4. Ciber escudos y secretos digitales

4.1 La LOPD y su aplicación en el ámbito educativo

En el bloque '**La LOPD y su aplicación en el ámbito educativo**', nos adentramos en el marco legal y práctico de la protección de datos personales, centrando nuestra atención en la **Ley Orgánica de Protección de Datos (LOPD)** y su esencial aplicación en el ámbito educativo. Comprenderemos los principios básicos de la protección de datos, explorando cómo estos se integran y se aplican para resguardar la información y los derechos del alumnado y profesorado.

A través de este bloque, aprenderás a implementar medidas de seguridad efectivas que garanticen la **integridad y la confidencialidad** de los datos dentro del entorno escolar.



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)



Pilares de la seguridad de la información



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<http://creativecommons.org/licenses/?lang=es>)

revisaremos los **derechos** que la LOPD garantiza a cada individuo, permitiendo un control más efectivo sobre su propia información. Finalmente, profundizaremos en el manejo adecuado de datos sensibles en el ámbito educativo.

En este apartado, '**Pilares de la seguridad de la información**', exploraremos los cimientos sobre los que se construye la seguridad de la información personal, en consonancia con la **Ley Orgánica de Protección de Datos** (LOPD).

Definiremos qué se considera **datos personales** y abordaremos los principios esenciales que deben regir su **tratamiento**. Además, discutiremos la importancia del **consentimiento** del interesado, un pilar fundamental para el tratamiento de datos personales, y

Objetivos:

- Entender los principios básicos de protección de datos según la LOPD.
- Desarrollar habilidades prácticas para implementar medidas de seguridad efectivas que garanticen la integridad y confidencialidad de los datos en entornos escolares.

Lecturas recomendadas:

- **Principios generales de la protección de datos**
<https://protecciondatos-lopd.com/empresas/principios-generales/>
(Atico34). Un recurso detallado que explica los principios fundamentales que rigen la protección de datos personales bajo la normativa europea.

- **La AEPD recibe el mayor número de reclamaciones en su historia** <<https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-recibe-por-tercer-anno-consecutivo-mayor-numero-reclamaciones-historia>> (AEPD). Noticia que destaca el incremento de las reclamaciones recibidas por la Agencia Española de Protección de Datos, reflejando la creciente preocupación por la privacidad.

A continuación, exploramos los principios básicos de la protección de datos, desde reconocer qué son los datos personales hasta implementar protocolos rigurosos para su protección y tratamiento adecuado.

- **Definición de datos personales.** Los datos personales se refieren a cualquier información que pueda identificar directa o indirectamente a una persona física, incluyendo nombres, direcciones, números de identificación, y elementos como la ubicación o identificadores en línea.
- **Principio de calidad de los datos.** El principio de calidad de los datos establece que la información personal debe ser precisa, actualizada y relevante para la finalidad para la que se recopila.
- **Consentimiento del titular.** El consentimiento para el tratamiento de datos debe ser informado, explícito y revocable, asegurando que los titulares entiendan su uso y puedan retirar su consentimiento en cualquier momento.
- **Finalidad del tratamiento.** Los datos personales deben utilizarse exclusivamente para fines específicos declarados al recogerlos, y cualquier cambio requiere nueva autorización por parte de los titulares.
- **Seguridad de los datos.** Implementar medidas de seguridad efectivas, tanto técnicas como organizativas, es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los datos.

- **Especial consideración de datos sensibles.** Algunos de los datos personales son especialmente sensibles por revelar circunstancias o información de las personas sobre su esfera más íntima y personal. Requieren que se les preste una especial atención y se adopten las medidas técnicas y organizativas necesarias para evitar que su tratamiento origine lesiones en los derechos y libertades de los titulares de los datos. Forman parte de esta categoría de datos personales aquellos que:
 - revelen ideología, afiliación sindical, religión y creencias.
 - hagan referencia al origen racial, a la salud y a la vida sexual.
 - se refieran a la comisión de infracciones penales o administrativas.
 - datos biométricos y genéticos.



Actividad (opcional): Reflexiones sobre la protección de datos

Descripción: Reflexiona sobre el manejo de datos personales en el ámbito educativo mediante preguntas clave que te ayudarán a entender mejor la aplicación de la LOPD.

Pasos:

1. Reflexiona y responde: ¿Dónde están los datos de mi alumnado?
2. ¿Puedo usar cualquier aplicación libremente?
3. ¿Quién tiene la responsabilidad sobre los datos?
4. Si quiero comunicarme con mi alumnado, ¿qué opciones tengo?
5. ¿Puedo realizar fotografías o vídeos sin consentimiento?

Recursos necesarios:

- Acceso al foro del curso para compartir respuestas.



Sus datos, nuestra responsabilidad



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En el ámbito educativo, la protección de los datos personales del alumnado no solo es una obligación legal, sino también una responsabilidad ética. Este apartado, '**Sus datos, nuestra responsabilidad**', se enfoca en cómo el profesorado y los centros educativos deben manejar los **datos personales**, desde su recogida hasta su **tratamiento** adecuado, asegurando siempre la **privacidad y seguridad**.

Cubriremos aspectos clave como la legitimación para el tratamiento de datos, la recogida

y manejo de imágenes del alumnado, la videovigilancia y el uso de datos en internet. También proporcionaremos un decálogo de buenas prácticas para asegurar que estos procesos se llevan a cabo de manera responsable y conforme a la ley.

Objetivos:

- Entender la legislación y responsabilidad ética del tratamiento de los datos personales del alumnado en el entorno educativo.
- Aplicar buenas prácticas para garantizar la integridad y privacidad de la información académica.

Lecturas recomendadas:

- **Guía breve sobre el GDPR para escuelas y profesorado** <<https://school-education.ec.europa.eu/en/insights/tutorials/brief-guide-gdpr-schools-and-teachers?prefLang=es>> (European School Education Platform). Un recurso ofrecido por la Unión Europea que proporciona una introducción al GDPR para el personal educativo.
- **Brechas de seguridad en el sector educación** <<https://haycanal.com/noticias/11774/brechas-de-seguridad-en-el-sector-educacion>> (Haycanal). Artículo que aborda los retos de la seguridad informática en el sector educativo y la importancia de proteger la información.

En España, la **edad mínima** para prestar **consentimiento** para el tratamiento de datos personales es de **14 años**, de acuerdo con el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). A partir de los 14 años, los menores de edad pueden otorgar su consentimiento para el tratamiento de sus datos personales. Para menores de esa edad el otorgamiento lo deberán dar sus padres, madres o tutores según el art. 7 LOPDGDD.

La Ley de Educación legitima a los centros educativos a recabar datos de carácter personal para la función docente y orientadora del alumnado en referencia a:

- El origen y ambiente familiar y social.
- Las características o condiciones personales.
- El desarrollo y resultados de su escolarización.
- Las circunstancias cuyo conocimiento sea necesario para educar y orientar al alumnado.

A tener en cuenta:

- Los datos personales no podrán usarse para fines diferentes al educativo (función docente y orientadora).
- El personal que acceda a los datos personales está sometido al deber de guardar secreto art.5 LOPDGDD.

Si se recogieron datos para realizar la matrícula, no se podrán utilizar para finalidades diferentes del ejercicio de la función educativa, como la publicación de fotografías del alumnado en la web del centro o la comunicación de sus datos a museos o empresas para organizar visitas, salvo que se haya recabado el consentimiento del alumnado o de sus padres, madres o tutores tras haberles informado de ello.

Preguntas frecuentes sobre la recogida de datos en centros educativos:

- **¿Se pueden recabar datos sobre la situación familiar de los padres, madres o tutores del alumnado?** Sí, los centros educativos pueden recabar la información sobre la situación familiar del alumnado. Esta información debe estar actualizada y los progenitores han de informar a los centros sobre cualquier modificación.
- **¿Se pueden recabar datos de salud?** Sí, en la medida en que sean necesarios para el ejercicio de la función educativa.
- **¿Se pueden recabar datos biométricos?** La recogida de datos debe ser proporcionada y no excesiva, garantizando siempre la seguridad y la privacidad. La Agencia Española de Protección de Datos prohíbe la recolección de datos biométricos de los estudiantes, salvo para el control de acceso a servicios como el comedor en instituciones con una gran cantidad de alumnado.

- **¿Se pueden recabar imágenes del alumnado para el expediente académico?** Sí, las fotografías se pueden incluir en expedientes académicos sin necesidad de consentimiento.
- **¿Se pueden recabar datos para finalidades distintas de la función educativa?** Sí, pero se necesita el consentimiento previo para finalidades como participar en concursos o actividades deportivas.
- **¿Puede un centro educativo acceder al contenido de dispositivos electrónicos del alumnado?** Requiere consentimiento, salvo en situaciones donde prevalezca el interés público o de seguridad del alumnado.

Preguntas frecuentes sobre el tratamiento de los datos del alumnado:

- **¿Se pueden hacer públicas las calificaciones escolares?** Se han de facilitar al propio alumnado y a sus padres, madres o tutores. En el caso de comunicar las calificaciones a través de plataformas educativas, éstas sólo deberán estar accesibles para el alumnado, sus padres, madres o tutores, sin que puedan tener acceso a las mismas personas distintas.
- **¿Puede el profesorado facilitar las calificaciones oralmente en clase?** No hay una prohibición expresa, pero se debe considerar la privacidad del alumnado.
- **¿Pueden los padres, madres o tutores solicitar las calificaciones de sus hijos mayores de edad?** Los padres, madres o tutores pueden solicitar las calificaciones de sus hijos mayores de edad si éstos corren con los gastos educativos o de manutención, existiendo un interés legítimo por parte de estos.
- **¿Pueden los padres, madres o tutores acceder a la información sobre las ausencias escolares de sus hijos mayores de edad?** La respuesta es

similar a la anterior; los padres, madres o tutores pueden tener acceso si corren con los gastos de manutención y existe un interés legítimo en la formación y educación de los hijos.

- **¿Acceso a la información académica por padres, madres o tutores separados?** Independientemente del estado civil de los padres, madres o tutores, ambos tienen derecho a acceder a la información académica de sus hijos, a menos que exista una resolución judicial que indique lo contrario. Los centros educativos deben establecer procedimientos para garantizar que el acceso a la información se haga respetando la legalidad vigente.
- **¿Se pueden comunicar los datos a instituciones, entidades o empresas que van a ser visitadas por el alumnado en una actividad extraescolar?** Sí, siempre que sea imprescindible para la actividad, y se cuente con el consentimiento de los padres, madres o tutores. La información que sobre estos eventos se facilita a los padres, madres o tutores para su autorización debe incluir la relativa a la comunicación de datos a estas entidades, así como la propia autorización.
- **¿Se pueden comunicar los datos a los Servicios Sanitarios autonómicos, o a un ayuntamiento para campañas de vacunación o programas de salud escolar (bucodental, alimentaria, etc.)?** Los centros deben trasladar a las familias la información para que éstas presten el consentimiento o faciliten los datos a los servicios de salud. Sin embargo, pueden facilitarse los datos del alumnado a los servicios de salud que los requieran sin necesidad de consentimiento en respuesta a una petición de las autoridades sanitarias, cuando los datos sean estrictamente necesarios para garantizar la salud pública.
- **¿Se pueden comunicar los datos del alumnado y de sus padres y madres a las AMPA?** No sin el previo consentimiento de los interesados. Las AMPA son responsables del tratamiento de los datos de carácter personal que hayan recabado, debiendo cumplir con la normativa de protección de datos en su tratamiento.

Preguntas frecuentes sobre el tratamiento de las imágenes del alumnado:

- **¿Pueden los centros educativos captar imágenes del alumnado durante las actividades escolares?** Sí, para funciones educativas. Para otros fines, como difusión, se requiere consentimiento .
- **¿Puede un profesor grabar imágenes del alumnado para una actividad escolar?** Sí, para uso interno educativo y no para difusión abierta .
- **¿Pueden los familiares del alumnado grabar imágenes del evento?** Sí, para uso personal y doméstico, pues en ese caso esta actividad está excluida de la aplicación de la normativa de protección de datos. Si las imágenes captadas por los familiares se difundieran, por ejemplo mediante su publicación en internet accesible en abierto, los familiares asumirían la responsabilidad.
- **Si unos padres, madres o tutores se niegan a que se tomen imágenes de su hijo, ¿se ha de cancelar el evento?** No. Se ha de informar a los padres, madres o tutores que la toma de fotografías y vídeos es posible como actividad familiar, exclusivamente para uso personal y doméstico, que está excluida de la aplicación de la normativa de protección de datos.
- **¿Pueden los centros escolares prohibir la toma de imágenes en sus instalaciones?** Sí, en base a su autonomía para establecer normas de organización.

Preguntas frecuentes sobre el tratamiento de los datos en internet:

- **¿Quién es el responsable del tratamiento de los datos en las plataformas educativas?** Los centros o las Administraciones educativas

que suscriben el contrato con las empresas de las plataformas educativas.

- **¿Estamos legitimados a usar cualquier plataforma educativa?** Sí, pero deben estar incluidas en la política de seguridad de los centros educativos, debiendo el profesorado solicitar, previamente a su utilización, la autorización.
- **¿Se pueden publicar en la web del centro los datos del profesorado?** Es necesario contar con su consentimiento previo si la web es de acceso público; si es interna, puede publicarse informando previamente.
- **¿Puede publicarse en la web del centro información relativa al alumnado?** Solo con el consentimiento del alumnado o sus representantes legales, o asegurándose que no se pueda identificar al alumnado, por ejemplo, pixelando las imágenes.

Preguntas frecuentes sobre la videovigilancia en los centros educativos:

- **¿Se pueden instalar cámaras de videovigilancia en todas las instalaciones del colegio?** No en todas las instalaciones. Dada la intromisión que supone en la intimidad de las personas, tanto del alumnado como del profesorado y demás personas cuya imagen puede ser captada por las cámaras, los sistemas de videovigilancia no podrán instalarse en aseos, vestuarios o zonas de descanso de personal docente o de otros trabajadores.
- **¿Se pueden instalar cámaras de videovigilancia en las aulas alegando motivos de conflictividad?** No, resultaría desproporcionado, pues durante las clases ya está presente el profesorado. Además de una intromisión en la privacidad del alumnado, podría suponer un control laboral desproporcionado del profesorado.

- **¿Se pueden instalar cámaras de videovigilancia en los patios de recreo y comedores?** Sí, siempre que exista una justificación válida y se respeten los principios de necesidad y proporcionalidad.
- **¿Se debe informar de la existencia de un sistema de videovigilancia?** Sí, colocando un distintivo en un lugar suficientemente visible en aquellos espacios donde se hayan instalado las cámaras. También se deberá disponer de una cláusula informativa que incluya los puntos exigidos por la normativa.

A continuación, os presentamos un conjunto de principios básicos que todo docente debería tener siempre en mente:

1. **Necesitamos sus datos personales.** Los centros educativos necesitan datos del alumnado y sus familias para ejercer su función, comprometiéndose a tratarlos con la máxima diligencia y respeto a su intimidad, siempre priorizando el interés y la protección de los menores.
2. **Estamos legitimados.** La gestión de datos por parte del centro está legitimada por la necesidad de realizar las tareas educativas y de administración sin necesitar el consentimiento expreso, pero manteniendo el deber de informar de manera comprensible y accesible.
3. **Con responsabilidad.** Las Administraciones y los centros educativos son los responsables del tratamiento de los datos y deben formar al profesorado sobre sus principios básicos y cómo tratar los datos correctamente.
4. **Informando de cada acción.** Se debe obtener consentimiento e informar cuando los datos se usen para fines distintos a los educativos, permitiendo la oposición a dicho uso.

- 5. Pidiendo permiso para el uso de aplicaciones.** Las TIC son herramientas fundamentales para la gestión y el aprendizaje del alumnado. Las Administraciones educativas y los centros deben conocer las aplicaciones que vayan a utilizar, su política de privacidad y sus condiciones de uso de éstas antes de utilizarlas, debiendo rechazarse las que no ofrezcan garantías.
- 6. El centro debe disponer de una guía.** Las Administraciones educativas y los centros deben establecer guías claras para el uso de tecnologías por parte del profesorado, adecuándolas al desarrollo de los estudiantes.
- 7. Comunicaciones por canales oficiales.** La interacción entre el profesorado y las familias del alumnado debe realizarse a través de canales oficiales como las plataformas del centro y el correo electrónico institucional.
- 8. No se recomienda el uso de Whatsapp.** Se desaconseja el uso de aplicaciones de mensajería como WhatsApp, a menos que sea necesario para proteger el interés superior del menor en situaciones urgentes.
- 9. Grabar sí difundir NO.** Podemos grabar imágenes y vídeos para uso educativo, pero nunca difundirlos sin consentimiento previo.
- 10. ¿Evento escolar? Avisemos a las familias de la NO difusión.** Al organizar eventos escolares, es práctica recomendable informar sobre las limitaciones en la captura y difusión de imágenes para respetar la vida privada de las personas involucradas.



Para garantizar un manejo adecuado de la información y cumplir con las normativas de protección de datos, es fundamental que los centros educativos se apoyen en recursos actualizados y fiables. A continuación, se

presentan tres guías imprescindibles que ofrecen orientación detallada y prácticas recomendadas en la gestión de datos en el ámbito educativo:

- **Guía para centros educativos** <<https://www.aepd.es/documento/guia-centros-educativos.pdf>> (AEPD). Un recurso esencial de la Agencia Española de Protección de Datos (AEPD) para comprender la aplicación de la protección de datos en el entorno educativo.
- **Informe sobre la utilización de aplicaciones en nube** <<https://www.aepd.es/guias/guia-orientaciones-apps-datos-alumnos.pdf>> (AEPD). Un informe de la AEPD en el que analiza el uso de aplicaciones que usan almacenamiento en la nube, en el ámbito educativo.
- **Guía de Protección de Datos para centros educativos** <<https://www.juntadeandalucia.es/educacion/portals/delegate/content/3fecd70c-8fa1-469d-8fb4-d09523f83882/Gu%C3%A3da%20LOPD%20Centros%20Educativos>> (Consejería de Desarrollo Educativo y Formación Profesional de la Junta de Andalucía). Una guía que detalla la protección de datos personales y las obligaciones de los centros educativos en Andalucía.

Actividad (opcional): Elaboración del decálogo de buenas prácticas

Descripción: En esta actividad, los participantes tendrán la oportunidad de aplicar los conocimientos adquiridos en este bloque de contenido sobre protección de datos en el entorno educativo. El desafío consistirá en elaborar tu propio decálogo de buenas prácticas para el tratamiento de datos personales en el ámbito escolar.

Pasos:

1. Reflexionar sobre los aspectos clave del tratamiento de datos personales en el contexto educativo.
2. Identificar las prácticas más relevantes y efectivas para garantizar la protección de la privacidad y seguridad de los datos del alumnado.
3. Elaborar un decálogo claro y conciso que incluya estas prácticas.
4. Compartir el decálogo elaborado en el foro del curso, explicando brevemente cada punto y su importancia.
5. Participar activamente en la discusión y retroalimentación de los decálogos de otros participantes.

Recursos necesarios:

- Materiales del curso sobre protección de datos en el ámbito educativo.
- Ejemplos de decálogos de buenas prácticas en otros contextos.
- Acceso al foro del curso para compartir el decálogo elaborado y participar en la discusión.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <<http://creativecommons.org/licenses/by-sa/4.0/>>

Módulo 4. Ciber escudos y secretos digitales

4.2 Protección de menores en línea

En el bloque '**Protección de menores en línea**', nos centraremos en desarrollar y fortalecer las estrategias para salvaguardar a los más jóvenes en el universo digital. Este segmento del curso subraya la importancia de utilizar **herramientas de control parental** y su correcta implementación en dispositivos educativos, proporcionando una barrera efectiva contra contenidos inapropiados y contactos peligrosos.

Además, abordaremos las **estrategias de prevención del ciberbullying**. A través de este bloque, no solo aprenderás a manejar herramientas técnicas, sino también a fomentar un entorno digital seguro y respetuoso para todos los estudiantes.



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)



El papel del control parental en la educación digital

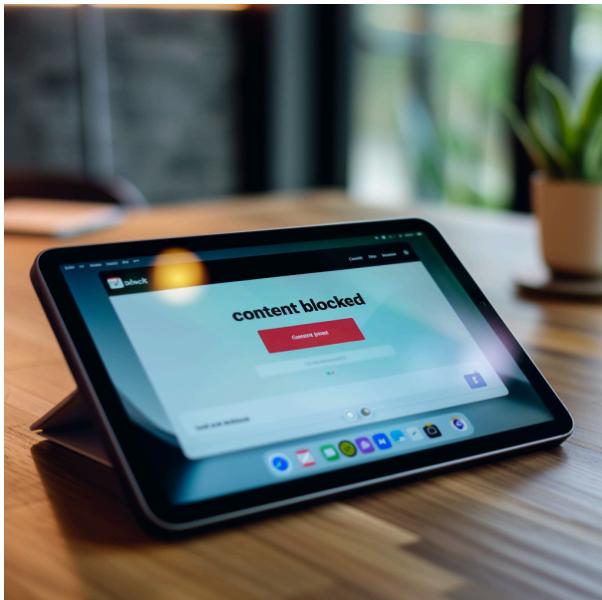


Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

potencialmente peligrosos.

En este apartado, exploraremos la importancia de utilizar y configurar adecuadamente estas herramientas para garantizar un **entorno educativo seguro** y propicio para el aprendizaje de los estudiantes.

Objetivos:

- Explorar y comprender la importancia de las herramientas de control parental en dispositivos educativos para crear un entorno seguro.
- Desarrollar habilidades para configurar y utilizar adecuadamente estas herramientas para proteger a los estudiantes de contenido no deseado y contactos peligrosos.

Lecturas Recomendadas:

- **Beneficios de los controles parentales**
<https://www.dongee.com/tutoriales/controles-parentales-beneficios/>
(Dongee). Un artículo que explica cómo los controles parentales pueden

El uso de dispositivos tecnológicos ha revolucionado la forma en que los estudiantes acceden a la información y participan en actividades de aprendizaje.

En este contexto, la implementación de **herramientas de control parental** en dispositivos educativos cobra una relevancia fundamental. Estas herramientas no solo actúan como una barrera efectiva contra el acceso a **contenido no deseado**, sino que también proporcionan una capa adicional de protección al limitar la interacción con contactos

proteger a los menores en línea y los beneficios de su uso adecuado en dispositivos tecnológicos.

- **Investigación sobre seguridad en internet y menores** <https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1989-709X2023000300005&lng=es&nrm=iso> (Scielo). Estudio detallado sobre el impacto de las medidas de seguridad en internet en la protección de los menores, incluyendo el uso de controles parentales.

Uno de los aspectos clave en la configuración de las herramientas de control parental es la adaptación a las edades y niveles de madurez de los estudiantes. Los controles deben ser más **restrictivos para los más jóvenes**, bloqueando contenidos inapropiados como violencia o material sexual, y pueden **relajarse gradualmente** para fomentar la autonomía en estudiantes mayores, siempre equilibrando protección y aprendizaje.

Además de la adaptación por edades, es importante personalizar las herramientas de control parental en función de las actividades educativas específicas que se desarrollen en cada centro. Esto implica **identificar** y permitir el acceso a los **recursos digitales necesarios** para el aprendizaje, al

mismo tiempo que se bloquean aquellos que puedan resultar perjudiciales o distractores.

Por ejemplo, en el caso de una clase de informática, quizás nos interesa permitir el acceso a plataformas de programación o diseño, mientras que se bloquean las redes sociales o los juegos en línea. De esta manera, se garantiza que los estudiantes puedan acceder a los contenidos y herramientas necesarias para su desarrollo académico, sin verse expuestos a riesgos innecesarios.

La configuración de las herramientas de control parental no es un proceso estático y requiere revisiones y actualizaciones constantes. Esto asegura su adaptación a las cambiantes necesidades del alumnado y a la evolución de los riesgos digitales. Un **monitoreo periódico** y ajustes adecuados mantienen estas herramientas efectivas y pertinentes, equilibrando protección con acceso a recursos educativos valiosos, y fomentando hábitos digitales saludables y responsables.

Es importante **educar a los estudiantes** sobre las herramientas de control parental, explicando su importancia, funcionamiento y los beneficios para su seguridad digital. Involucrar activamente a los estudiantes promueve una **cultura de uso responsable** de la tecnología y los empodera como agentes de su propia seguridad digital.

También es esencial mantener una **comunicación** abierta y transparente con las **familias**, informándoles sobre estas herramientas y colaborando en su configuración. Esta colaboración **fomenta un entorno de confianza** y asegura el desarrollo saludable de los estudiantes en el entorno digital.

La elección de herramientas de control parental depende de múltiples factores como el tipo de control necesario, el dispositivo y el sistema operativo en uso. Dado que es complicado recomendar una única solución que se adapte a todas las necesidades, es esencial ofrecer recursos que permitan a cada usuario encontrar la opción más adecuada:

- **Guía de INCIBE sobre controles parentales** <https://files.incibe.es/is4k/is4k_guia_controles_parentales.pdf> : Esta guía ofrece un panorama de las herramientas disponibles para diferentes dispositivos, incluyendo filtrado de contenidos, control del tiempo, supervisión de actividad, geolocalización y protección de la configuración.
- **Catálogo de herramientas de control parental en INCIBE** <https://www.incibe.es/menores/familias/control-parental?field_herra_categoria_target_id>All&field_dispositivo_target_id>All&field_herra_gratuidad_target_id>All&field_field_herra_idioma_lista_value>All> : Enlace a categorías específicas de herramientas de control parental,

donde se puede obtener más información y descargar las aplicaciones según las necesidades.

- **Guía de mediación parental de INCIBE** <<https://www.incibe.es/menores/familias/mediacion-parental>> : Un recurso adicional que proporciona estrategias para una mediación efectiva en el uso de la tecnología por parte de los menores.

Seleccionar la herramienta adecuada requiere considerar cuidadosamente las características específicas de cada opción y cómo éstas se alinean con las necesidades del entorno educativo y familiar.



Actividad de debate (opcional): Herramientas de control parental en dispositivos educativos

Descripción: Reflexiona y debate sobre la presencia y la necesidad de herramientas de control parental en los dispositivos de los centros educativos.

- ¿Tu centro educativo utiliza herramientas de control parental en sus dispositivos?
- ¿Consideras necesarias estas herramientas? ¿Por qué sí o por qué no?
- ¿Sería posible coordinarse entre el equipo educativo para decidir qué recursos dejar disponibles y cuáles restringir?
- ¿Cómo se podría implementar una política de control parental que sea efectiva y respetuosa con la privacidad y autonomía de los estudiantes?

Pasos:

1. Reflexiona individualmente sobre las preguntas propuestas.
2. Participa en el foro del curso, compartiendo tus opiniones y leyendo las de tus compañeros.
3. Intenta llegar a conclusiones comunes sobre las políticas de control parental en el contexto educativo.

Recursos necesarios:

- Acceso al foro del curso.
- Documentos de política de TI de tu centro educativo, si están disponibles.



Ciberbullying: prevención y respuesta



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

En este apartado del curso, exploraremos de manera integral el ciberbullying, centrándonos en la prevención y la respuesta adecuada ante esta problemática. Desde la definición y los tipos, hasta las **medidas preventivas**. Nos sumergiremos en un enfoque educativo y proactivo para crear entornos escolares seguros y libres de acoso en línea.

En el entorno digital actual, el **ciberbullying** se ha convertido en una **preocupación creciente** en las escuelas, afectando a la seguridad y al **bienestar emocional** del alumnado. Como educadores, es fundamental comprender la naturaleza de este acoso, sus impactos devastadores y las estrategias efectivas para prevenir y abordar esta forma de acoso en línea.

Objetivos:

- Comprender la naturaleza del ciberbullying: Analizar los diferentes tipos de ciberbullying y sus impactos en la seguridad y bienestar emocional de los estudiantes.
- Desarrollar estrategias preventivas, promoviendo entornos escolares seguros y libres de acoso en línea.

Lecturas recomendadas:

- **Ciberacoso: ¿qué es y cómo detenerlo?** <<https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#1>> (UNICEF). Recurso que proporciona información sobre qué es el ciberacoso y cómo detenerlo, ofreciendo consejos prácticos y recursos para abordar esta problemática.
- **Estadísticas de ciberacoso** <<https://www.comparitech.com/es/proveedores-de-internet/estadisticas-ciberacoso/>> (Comparitech). Artículo que presenta estadísticas actuales sobre el ciberacoso, incluyendo datos sobre su prevalencia, tipos y consecuencias, proporcionando una visión general de la situación actual.

El ciberbullying, también conocido como ciberacoso o acoso a través de medios digitales, se define como el uso de tecnologías digitales, como redes sociales, mensajes de texto, correo electrónico y otras plataformas, con la intención de dañar, intimidar o acosar a otra persona. A diferencia del acoso tradicional, el ciberbullying se produce en un entorno virtual y puede tener un alcance mucho más amplio y duradero.

Características

- **Anonimato:** Los agresores pueden ocultar su identidad detrás de perfiles en línea, lo que les da un sentido de impunidad.
- **Alcance ilimitado:** El contenido dañino puede difundirse rápidamente y llegar a un gran número de personas.
- **Persistencia:** El material publicado en línea puede permanecer visible durante mucho tiempo, incluso después de que el acoso haya cesado.
- **Dificultad de supervisión:** Es más difícil para los padres, educadores y autoridades monitorear y controlar el comportamiento en línea.
- **Desinhibición:** La distancia física y la falta de contacto cara a cara pueden llevar a los agresores a comportarse de manera más agresiva y cruel.

Evolución

El ciberbullying ha evolucionado a medida que la tecnología y el uso de Internet se han expandido. En las últimas décadas, hemos visto un aumento significativo en la prevalencia y la gravedad de este fenómeno, especialmente entre los jóvenes. A medida que surgen nuevas plataformas y aplicaciones, los agresores encuentran formas cada vez más sofisticadas de acosar a sus víctimas.

El ciberbullying puede manifestarse de diversas **formas**, algunas de las más comunes incluyen:

- **Acoso en redes sociales:** Publicación de contenido denigrante, amenazas, burlas o rumores sobre la víctima en plataformas como Facebook, Instagram, Twitter, etc.

- **Mensajes de texto y aplicaciones de mensajería:** Envío de mensajes ofensivos, intimidatorios o acosadores a través de SMS, WhatsApp, Telegram y otras aplicaciones de mensajería.
- **Difusión de rumores y contenido dañino:** Creación y propagación de rumores falsos o información perjudicial sobre la víctima en línea.
- **Suplantación de identidad:** Hacerse pasar por la víctima en redes sociales o plataformas en línea para publicar contenido dañino.
- **Exclusión y aislamiento:** Bloquear o excluir deliberadamente a la víctima de grupos en línea o actividades virtuales.
- **Grabación y difusión de contenido humillante:** Grabar y compartir videos o imágenes comprometedoras de la víctima sin su consentimiento.
- **Acoso a través de juegos en línea:** Intimidación, amenazas o acoso dirigido a otros jugadores en entornos de juegos en línea.

Las plataformas y **medios** más utilizados para llevar a cabo el ciberbullying incluyen:

- Redes sociales (Facebook, Instagram, Twitter, TikTok, etc.)
- Aplicaciones de mensajería (WhatsApp, Telegram, Snapchat, etc.)
- Correo electrónico
- Foros y comunidades en línea
- Juegos en línea
- Sitios web y blogs
- Plataformas de alojamiento de videos (YouTube, Vimeo, etc.)

Estas formas y medios de ciberbullying aprovechan las características de anonimato, alcance ilimitado y persistencia de la información en línea, lo que dificulta la detección y la respuesta efectiva al problema.

Como educadores, tenemos un papel fundamental en la prevención del ciberbullying. A continuación, presentamos una serie de medidas en las que podemos ayudar a los adolescentes a protegerse y mantener un entorno en línea seguro.

- **Educación digital y alfabetización mediática:** Fomentar el pensamiento crítico sobre el contenido en línea y la identificación de información falsa o dañina.
- **Uso seguro de contraseñas:** Crear contraseñas seguras y únicas para cuentas en línea y evitar compartirlas.
- **Configuración de la privacidad:** Revisar y ajustar regularmente la configuración de privacidad en redes sociales y otras plataformas en línea.
- **Pensar antes de publicar:** Considerar el impacto de las publicaciones en línea antes de compartirlas.
- **Respeto en línea:** Evitar participar en conversaciones o acciones que puedan ser percibidas como hostiles o intimidatorias.
- **No compartir información personal:** Educar sobre la importancia de no compartir información personal en línea.
- **Bloqueo y reporte:** Enseñar cómo bloquear y reportar a usuarios que participen en comportamientos de ciberbullying.
- **Pausas digitales:** Promover el equilibrio entre el tiempo en línea y fuera de línea, alentando a tomar descansos para desconectar.

En las secciones de recursos educativos de los módulos anteriores hemos explorado una variedad de recursos para abordar en nuestras aulas las medidas que se plantean. Además, en la misma sección, recursos educativos, de este bloque de contenido, se incluyen recursos específicamente orientados a la prevención y concienciación del ciberbullying, proporcionando herramientas adicionales para abordar este importante tema en el entorno escolar.

Actividad práctica (opcional): ¿Conoces los riesgos a los que se enfrentan los menores en internet?

Descripción: Ponte a prueba con el test de autoevaluación diseñado por INCIBE para evaluar tu conocimiento sobre los riesgos a los que se enfrenta nuestro alumnado en internet. Accede al **siguiente enlace**

<<https://www.incibe.es/menores/tests/conoces-los-riesgos-los-que-se-enfrenta-tu-hijo-en-internet>> y realiza el test de autoevaluación.



Recursos educativos

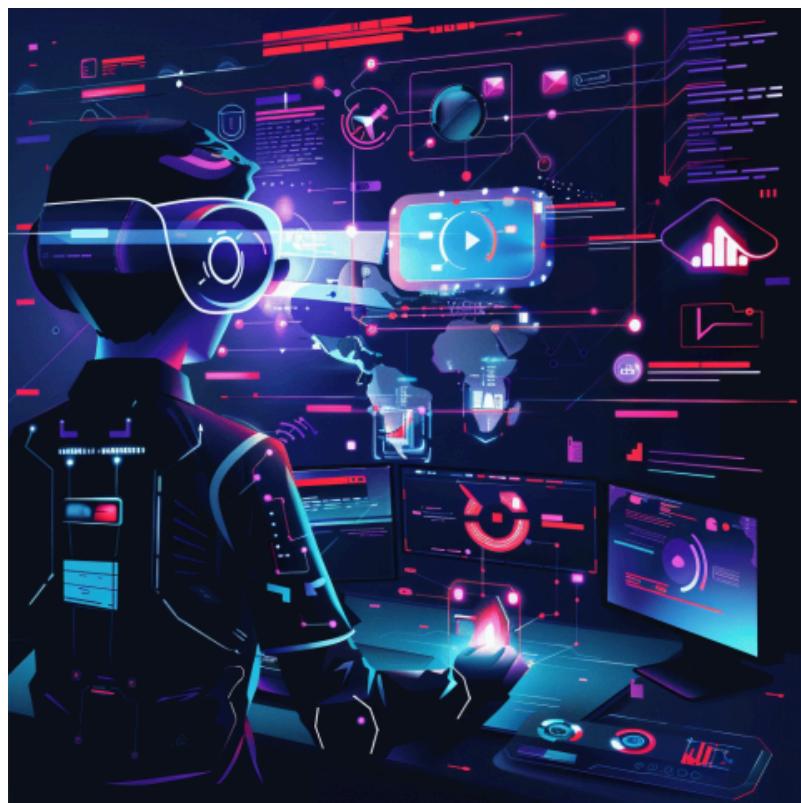


Imagen generada con IA (Midjourney) (CC BY-NC-SA
<<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>>)

Explora estos **recursos** para enseñar ciberseguridad: actividades, lecturas y más, diseñados para fomentar la **prevención y la acción contra el ciberacoso** entre nuestros estudiantes.

Infografías

- **Sabes actuar contra el ciberacoso:** Guía que proporciona estrategias y consejos para manejar situaciones de ciberacoso. [Ver guía <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_sabes_actuar_contra_el_ciberacoso.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_sabes_actuar_contra_el_ciberacoso.pdf).
- **Reconoce el ciberacoso a tiempo:** Infografía que ayuda a identificar señales de alerta temprana del ciberacoso. [Ver infografía <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_reconoce_el_ciberacoso_a_tiempo.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_reconoce_el_ciberacoso_a_tiempo.pdf).
- **En mi aula todos contra el ciberacoso:** Guía con estrategias para crear un entorno escolar seguro y libre de ciberacoso. [Ver guía <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_en_mi_aula.todos_contra_el_ciberacoso.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_en_mi_aula.todos_contra_el_ciberacoso.pdf).
- **Ciberacoso escolar. No comarto, no me gusta:** Infografía para fomentar la no participación en conductas de ciberacoso. [Ver infografía <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_ciberacoso_escolar_no_comparto_no_me_gusta.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_ciberacoso_escolar_no_comparto_no_me_gusta.pdf).

Juegos de mesa

- **Escalera de Internet:** Juego educativo para aprender a cómo actuar en internet, mostrando rechazo ante conductas ofensivas. [Enlace al juego <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_escalera_de_internet.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_escalera_de_internet.pdf).
- **Hablemos de ciberacoso:** Juego de tarjetas para reflexionar sobre el sobre el ciberacoso. [Enlace al juego <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_hablemos_de_ciberacoso.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_hablemos_de_ciberacoso.pdf).
- **La Oca del Ciberacoso:** Juego de mesa didáctico para aprender sobre el ciberacoso de forma interactiva. [Enlace al juego <https://www.incibe.es/menores/juegos/juegos-didacticos/oca>](https://www.incibe.es/menores/juegos/juegos-didacticos/oca).
- **Ahora te toca a ti:** Actividades para fomentar la empatía y la responsabilidad en el uso de las redes. [Enlace al juego <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_ahora_te_toca_a_ti.pdf>](https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_ahora_te_toca_a_ti.pdf).

Actividades interactivas

- **Cada comentario cuenta:** Material para sensibilizar sobre el impacto de las palabras en internet. **Enlace a la actividad** <https://www.incibe.es/sites/default/files/contenidos/materiales/Campañas/ciberacoso/is4k_cada_comentario_cuenta.pdf> .
- **Anatomía de una publicación en una red social:** Recurso educativo que desglosa los componentes de las publicaciones en redes y cómo pueden ser manipuladas. **Enlace a la actividad** <https://es.educaplay.com/recursos-educativos/18438464-anatomia_de_una_publicacion_en_una_red_social.html> .
- **Al otro lado de la pantalla:** Juego que ayuda a entender las consecuencias del ciberacoso desde la perspectiva de la víctima. **Acceder a la actividad** <https://es.educaplay.com/recursos-educativos/5851051-al_otro_lado_de_la_pantalla.html> .
- **En Internet con seguridad:** Juego interactivo que enseña a los menores cómo navegar de forma segura en Internet. **Enlace a la actividad** <https://es.educaplay.com/recursos-educativos/4286064-en_internet_con_seguridad.html> .
- **En Internet con respeto:** Juego interactivo que promueve el respeto y la buena convivencia en línea. **Enlace a la actividad** <https://es.educaplay.com/recursos-educativos/4284903-en_internet_con_respeto.html> .

Otros recursos

- **Dinámicas para prevenir conflictos en Instagram:** Recursos para trabajar en el aula con el objetivo de prevenir conflictos en redes sociales. **Enlace a la dinámica** <<https://www.incibe.es/menores/educadores/materiales-didacticos/recursos-para-trabajar-en-el-aula/dinamicas-para-prevenir-conflictos-en-instagram>> .
- **Vídeo de ciberacoso:** Vídeo que proporciona una perspectiva clara sobre el ciberacoso y sus efectos, fomentando la reflexión y la acción. **Ver vídeo** <<https://www.youtube.com/watch?v=1z0bKk5IfbU>> .

Módulo 4. Ciber escudos y secretos digitales

4.3 Más allá de las crisis digitales

En el bloque '**Más allá de las crisis digitales**', exploraremos el concepto de **resiliencia digital** y su crucial importancia en la protección de nuestros espacios educativos. Este segmento del curso se enfoca en **desarrollar la capacidad de adaptarse y recuperarse** de incidentes de ciberseguridad, asegurando que los procesos educativos puedan continuar sin interrupciones significativas.

Profundizaremos en cómo los docentes y las instituciones pueden construir una resiliencia efectiva, no solo a través de la teoría, sino también mediante la práctica de crear y mantener **copias de seguridad regulares** de datos importantes. A través de este bloque, aprenderás a implementar estrategias que fortalezcan la continuidad y la integridad de la educación, incluso en el contexto de desafíos digitales.



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)



Resiliencia digital en el ámbito educativo



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

su importancia crítica y ofreciendo estrategias prácticas para fortalecerla.

La resiliencia digital se refiere a la capacidad de las personas, organizaciones y sistemas para **anticipar, adaptarse y responder** de manera efectiva a los **desafíos y disruptores digitales**. En el contexto educativo, la resiliencia digital es fundamental para garantizar la continuidad y la calidad del proceso de enseñanza-aprendizaje, especialmente en un entorno cada vez más digitalizado.

En este apartado del curso, exploraremos a fondo el concepto de resiliencia digital en el ámbito educativo, destacando

Objetivos:

- Explorar la importancia de la resiliencia digital en el ámbito educativo y sus implicaciones para garantizar la continuidad del proceso de enseñanza-aprendizaje.
- Ofrecer una visión general de algunas medidas y prácticas que pueden contribuir a desarrollar la resiliencia digital en el contexto educativo.

Lecturas Recomendadas:

- Resiliencia Digital: Un Paso Más Allá de la Ciberseguridad
<https://www.csoonline.com/article/3293898/digital-resilience-a-step-up-from-cybersecurity.html#:~:text=Digital%20Resilience%20%E2%80%93%20an%20organization's%20ability,recover%20technology%2Ddependent%20operational%20capability.&text=Being%20digitally%20resilient%20means%20an,continued%20competitiveness%20and%20business>

%20survival.> (CSO Online). Este artículo explora la resiliencia digital como la capacidad de una organización para anticipar, adaptarse y recuperarse de incidentes digitales, destacando su importancia para la continuidad del negocio y la competitividad.

- **Ciberresiliencia: La Clave para Sobreponerse a los Incidentes** <<https://www.incibe.es/incibe-cert/blog/ciberresiliencia-la-clave-para-sobreponerse-los-incidentes>> (INCIBE). En este artículo se analiza la ciberresiliencia como un elemento esencial para enfrentar y superar incidentes de seguridad digital, ofreciendo perspectivas valiosas sobre cómo fortalecerla.

Cuando hablamos de resiliencia digital, es importante entender que este concepto va más allá de la mera ciberseguridad. Si bien, en el ámbito empresarial la resiliencia digital se refiere a la capacidad de una organización para mantener, cambiar o recuperar la capacidad operativa dependiente de la tecnología, en el contexto educativo adquiere una dimensión más amplia. En el campo de la educación, la resiliencia digital se entiende como la habilidad de individuos, instituciones y sistemas educativos para anticipar, adaptarse y responder eficazmente a los desafíos y disruptpciones tecnológicas.

Sin embargo, **en este curso** nos enfocaremos específicamente en la **perspectiva de la ciberseguridad en el ámbito educativo**, explorando cómo la resiliencia digital puede fortalecer la protección de datos sensibles y la **respuesta efectiva ante posibles incidentes**.

Para fortalecer la resiliencia digital en el ámbito educativo, es necesario implementar estrategias a nivel institucional, docente y estudiantil:

- **Nivel institucional**

- **Planes de continuidad y recuperación:** Establecer planes detallados para mantener la continuidad de las operaciones educativas y recuperarse eficazmente de incidentes digitales.
- **Inversión en infraestructura segura:** Priorizar la inversión en infraestructura y herramientas tecnológicas robustas y seguras para proteger los datos críticos.
- **Capacitación en competencias digitales:** Brindar formación continua en competencias digitales al personal docente y administrativo para fortalecer la seguridad en el uso de la tecnología.

- **Nivel docente**

- **Integración segura de tecnologías:** Enseñar a integrar de manera segura y efectiva las tecnologías en las actividades de enseñanza, priorizando la protección de la información.
- **Desarrollo de habilidades digitales:** Fomentar el desarrollo de habilidades para adaptarse e innovar en entornos digitales, promoviendo la seguridad como parte integral de la enseñanza.
- **Fomento de copias de seguridad:** Enseñar a los docentes la importancia de realizar copias de seguridad de manera regular para proteger la información educativa y garantizar la continuidad de las actividades en caso de incidentes.

- **Nivel estudiantil**

- **Fomento de competencias digitales:** Promover el desarrollo de competencias digitales y de pensamiento crítico entre los estudiantes, enfatizando la importancia de la seguridad en línea.
- **Enseñanza de prácticas seguras:** Educar sobre estrategias de uso seguro y responsable de las tecnologías, inculcando hábitos que protejan la privacidad y la integridad de los datos.

- **Promoción de la autonomía y adaptabilidad:** Impulsar la autonomía y la adaptabilidad de los estudiantes en entornos digitales, preparándolos para enfrentar desafíos de seguridad de manera proactiva.

Al examinar los puntos relacionados con los docentes y estudiantes, podemos observar que todos han sido abordados y fortalecidos a lo largo del curso. Sin embargo, aún queda un aspecto crucial por cubrir: las **copias de seguridad**. En el siguiente apartado, nos enfocaremos en este aspecto fundamental de la resiliencia digital en el ámbito educativo.

Nota: Si bien la parte institucional desempeña un papel fundamental en la resiliencia digital, su tratamiento queda fuera del alcance y los objetivos específicos de este curso.

Actividad (opcional): Evaluando mi resiliencia digital

Descripción: Luis es un docente entusiasta que prepara clases interactivas utilizando una variedad de recursos digitales. Un día, al encender su ordenador, descubre con horror que no puede acceder a su información, todos sus archivos están cifrados por un ransomware. Su presentación para la próxima clase, sus apuntes, incluso sus contactos y calendario están inaccesibles. En ese momento se da cuenta de que sin acceso a esos recursos digitales, sus lecciones planificadas se han vuelto completamente inutilizables.

Pasos:

1. Imagina que eres tú el protagonista de esta historia y considera cómo te enfrentarías a esta situación desde tu propia experiencia como docente.
2. Reflexiona sobre cómo afectaría la interrupción de tus actividades educativas si no pudieras acceder a tus recursos digitales.
3. Considera qué medidas de seguridad podrías haber implementado previamente para prevenir o mitigar el impacto de un ataque de ransomware.
4. Analiza cómo una estrategia efectiva de copias de seguridad podría haber ayudado a recuperar tus datos y minimizar el tiempo de inactividad.

Recursos necesarios:

- Tiempo para reflexionar sobre la situación planteada.



Resguardando el conocimiento



Imagen generada con IA (Midjourney)
(CC BY-NC-SA
<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>)

prácticas para su implementación efectiva.

La realización de copias de seguridad es una práctica imprescindible en ciberseguridad, especialmente en el ámbito educativo. Ante la **creciente amenaza de ataques** cibernéticos, como el ransomware, que pueden comprometer la integridad y disponibilidad de los datos, la implementación de copias de seguridad se vuelve necesaria.

En este apartado, exploraremos en detalle la **importancia** de las **copias de seguridad** en el contexto educativo y proporcionaremos **estrategias**

Objetivos:

- Comprender la importancia de las copias de seguridad en el ámbito educativo.

- Proporcionar estrategias prácticas para la implementación efectiva de copias de seguridad.

Lecturas recomendadas:

- **¿Qué es una copia de seguridad 3-2-1 y cómo protege nuestros datos?** <<https://www.redeszone.net/tutoriales/seguridad/copia-seguridad-3-2-1-proteger-datos/>> (RedesZone). Un artículo que presenta la regla de copia de seguridad 3-2-1 y su importancia para proteger la información contra la pérdida de datos.
- **Definiendo mi estrategia de copias de seguridad** <<https://www.incibe.es/ciudadania/blog/definiendo-mi-estrategia-de-copias-de-seguridad>> (INCIBE). En este artículo se proporcionan consejos y pautas para definir una estrategia efectiva de copias de seguridad que garantice la protección de la información crítica.

Los docentes son responsables de generar y gestionar una gran cantidad de información educativa crítica, como planes de estudio, materiales de enseñanza, registros de calificaciones y evaluaciones del alumnado. La pérdida o el daño de estos datos puede tener un impacto significativo en el proceso de enseñanza-aprendizaje. Las copias de seguridad regulares garantizan que esta información pueda ser recuperada y restaurada en caso de incidentes digitales, ciberataques o desastres naturales.

Por ello, es imprescindible contar con un sistema de copias de seguridad. Esto implica:

- Realizar **respaldos periódicos** de la información.
- Almacenar las copias de seguridad en **ubicaciones seguras y redundantes**.

- **Probar la restauración** de los datos para asegurar la integridad y la disponibilidad de la información.

La regla del 3, 2, 1 es una estrategia simple pero efectiva para realizar copias de seguridad de manera segura y confiable. ¿En qué consiste esta pauta a la hora de realizar copias de seguridad?

- **3 copias de tus datos:** Mantén al menos tres copias de tus datos importantes, el original con el que estás trabajando más dos copias.
- **2 dispositivos de almacenamiento diferentes:** Guarda estas copias en al menos dos tipos diferentes de dispositivos de almacenamiento. Por ejemplo, puedes tener una copia en tu ordenador (copia con la que trabajas), otra en un disco duro externo y una tercera en la nube.
- **1 copia fuera del sitio:** Asegúrate de que al menos una de tus copias de seguridad esté almacenada externamente.

La importancia de esta estrategia se resume en los siguientes puntos:

- **Resiliencia y redundancia:** Al seguir esta regla, se garantiza la disponibilidad de los datos incluso en situaciones de pérdida o corrupción de información.
- **Protección contra ransomware y desastres:** Al tener una copia fuera del sitio, se evita la posibilidad de que los datos se vean comprometidos por ataques de ransomware o desastres que afecten el sitio principal.
- **Cumplimiento normativo:** Esta estrategia cumple con muchos estándares de seguridad y normativas que exigen la protección y disponibilidad de los datos.

Actividad (opcional): Desarrollo de un plan de copias de seguridad personalizado

Descripción: Elabora un plan de copias de seguridad adaptado a tus necesidades como docente para proteger tus materiales educativos y garantizar la disponibilidad de la información en caso de pérdida o daño.

Pasos:

1. Evalúa tus materiales educativos: Identifica los documentos, presentaciones, recursos multimedia y cualquier otro material digital que utilices en tu trabajo como docente.
2. Identifica los riesgos: Considera posibles escenarios de pérdida de datos, como fallas en el dispositivo, ataques de malware o errores humanos.
3. Elige el método de respaldo: Decide si prefieres utilizar almacenamiento local (discos duros externos, memorias USB) o almacenamiento en la nube (Google Drive, Dropbox).
4. Establece la frecuencia de respaldo: Determina con qué frecuencia realizarás copias de seguridad, basándote en la frecuencia de creación o modificación de tus materiales.
5. Implementa el plan: Configura las herramientas necesarias para realizar las copias de seguridad de acuerdo con tu plan establecido.
6. Prueba la recuperación: Asegúrate de que puedas acceder y restaurar tus datos desde las copias de seguridad realizadas, realizando pruebas periódicas de recuperación.

Recursos necesarios:

- Acceso a un dispositivo de almacenamiento (disco duro externo, memoria USB).
- Acceso a servicios de almacenamiento en la nube, si decides utilizar esta opción.
- Herramientas de respaldo y recuperación de datos, como software de copias de seguridad o aplicaciones en línea.

Obra publicada con **Licencia Creative Commons Reconocimiento Compartir igual 4.0** <<http://creativecommons.org/licenses/by-sa/4.0/>>

Módulo 4. Ciber escudos y secretos digitales

4.4 Actividades obligatorias



Imagen generada con IA (Ideogram) (CC BY-NC-SA
<http://creativecommons.org/licenses/?lang=es>)



Actividad 4.1: Análisis de casos prácticos

Descripción: Esta actividad se centra en investigar y analizar resoluciones sancionadoras emitidas por la Agencia Española de Protección de Datos (AEPD) a centros educativos. El objetivo es

comprender mejor la aplicación de las normativas de protección de datos en el entorno educativo. Deberás reflexionar y compartir tus opiniones en el foro del curso sobre el caso que estudies.

Pasos:

- Accede al buscador de la AEPD a través del siguiente enlace, ya pre-filtrado, para ver resoluciones en el ámbito educativo: **Buscador de resoluciones de la AEPD - sector educativo** https://www.aepd.es/informes-y-resoluciones/resoluciones?search_api_fulltext=&sort_bef_combine=fecha_firma_DESC&f%5B0%5D=sectorial%3A2422.
- Revisa algunas de estas resoluciones y selecciona una para analizar en profundidad.
- Reflexiona sobre las implicaciones y aprendizajes que se pueden extraer de la resolución elegida.
- Comparte tus reflexiones en el foro del curso, incluyendo:
 - Análisis del caso seleccionado, detallando los hechos, la resolución de la AEPD, y las sanciones impuestas, si las hay.
 - Tu opinión sobre las acciones que llevaron al centro educativo a recibir una sanción y propuestas de medidas de mejora para evitar futuras sanciones.
 - Comentarios a las contribuciones de tus compañeros/as, ofreciendo tu perspectiva. Asegúrate de responder al menos a una entrada del foro para promover la interacción y el intercambio de ideas.

Recursos necesarios:

- Acceso a internet.
- Enlaces a las resoluciones de la AEPD.

Rúbrica actividad 4.1 *Aplicar*

	Nivel alto	Nivel medio	Nivel bajo
Análisis detallado del caso	Análisis exhaustivo del caso seleccionado, incluyendo detalles completos sobre los hechos, resolución y sanciones impuestas. (2.5)	Análisis parcial que menciona algunos detalles importantes del caso, pero omite otros. (1.25)	No se ha realizado el análisis del caso. (0)
Reflexión crítica sobre el caso	Reflexión profunda sobre las implicaciones del caso, con propuestas claras y fundamentadas para mejorar la situación. (2.5)	Reflexión que identifica aspectos generales, con propuestas de mejora poco específicas o incompletas. (1.25)	No se ha incluido reflexión crítica sobre el caso. (0)
Interacción en el foro	Participación activa en el foro con aportaciones constructivas y respuesta a	Participación limitada en el foro con poca interacción con las	No participa o interactúa

	Nivel alto	Nivel medio	Nivel bajo
	al menos una entrada de otro compañero/a. (2.5)	entradas de los compañeros/as. (1.25)	mínimamente en el foro. (0)
Aplicación de aprendizajes	Demuestra una comprensión profunda de las normativas y aplica los aprendizajes de manera clara y relevante en sus propuestas. (2.5)	Muestra comprensión de las normativas, pero las aplicaciones o propuestas son generales o poco profundas. (1.25)	No se ha aplicado los aprendizajes relacionados con las normativas. (0)



Actividad 4.2: Infografía sobre prevención del ciberbullying

Descripción: En esta actividad crearás una infografía informativa y visualmente atractiva que aborde las medidas y acciones preventivas contra el ciberbullying que pueden implementarse en el aula y en entornos digitales.

Pasos a seguir:

1. Analiza los materiales sobre el ciberbullying y las mejores prácticas para prevenirlo en el contexto escolar trabajados en el módulo.
2. Identifica las pautas y actuaciones más efectivas para prevenir el ciberbullying en el aula y en entornos digitales. Considera aspectos como la promoción de la empatía, el fomento de la comunicación abierta, la supervisión activa en línea y la enseñanza de habilidades digitales responsables.
3. Organiza la información de manera clara y concisa, utilizando iconos, imágenes y texto para transmitir tus mensajes de manera efectiva, acorde a la edad de tu alumnado.
4. Asegúrate de incluir recomendaciones específicas para el profesorado y para los alumnos, destacando acciones concretas que puedan implementarse en el aula y en actividades digitales.
5. Recuerda incluir tu nombre/nick/alias y la licencia de uso. Puedes consultar el sitio web de **Creative Commons <https://chooser-beta.creativecommons.org/?lang=es_ES>** para elegir la licencia.
6. Puedes entregar la infografía en pdf o un enlace público a la misma.
7. Reflexiona sobre el proceso de creación de la infografía y evalúa la efectividad de tus mensajes. Considera cómo podrían utilizarse estas infografías como herramientas educativas en el aula y cómo podrían contribuir a la prevención del ciberbullying.

Recursos necesarios:

- Canva, Genially, Presentaciones de Google u otras herramientas de diseño gráfico.
- Materiales sobre el ciberbullying y las mejores prácticas para prevenirlo.
- Iconos, imágenes y texto relevantes para la creación de la infografía.

Recursos adicionales:

Aquí tienes algunas fuentes donde puedes encontrar imágenes, iconos y plantillas gratuitas para tu infografía:

- Freepik: Freepik ofrece una amplia variedad de recursos gráficos gratuitos, como iconos, ilustraciones y plantillas de infografías. Puedes explorar su colección y descargar elementos para tu diseño en: [Freepik <https://www.freepik.com/>](https://www.freepik.com/) .
- Canva: Canva es una plataforma en línea que proporciona herramientas para diseñar infografías de manera sencilla y profesional. Ofrece una amplia gama de plantillas gratuitas y elementos gráficos para personalizar tu diseño. Puedes acceder a Canva en: [Canva <https://www.canva.com/>](https://www.canva.com/) .
- Pexels: Pexels es un banco de imágenes gratuitas de alta calidad que puedes utilizar en tu infografía. Ofrece una amplia variedad de fotos libres de derechos de autor que puedes descargar y utilizar en tus diseños. Explora la colección en: [Pexels <https://www.pexels.com/>](https://www.pexels.com/) .
- Flaticon: Flaticon es una plataforma que ofrece una gran variedad de iconos gratuitos en formato vectorial. Puedes buscar y descargar iconos relacionados con la prevención del ciberbullying para incluir en tu infografía. Encuentra más información en: [Flaticon <https://www.flaticon.com/>](https://www.flaticon.com/) .
- Generación de imágenes con inteligencia artificial: Se recomienda utilizar modelos de inteligencia artificial de código abierto para generar imágenes. Por ejemplo, [Ideogram <https://ideogram.ai/>](https://ideogram.ai/) es un modelo gratuito que puede generar imágenes con texto. Aquí tienes un ejemplo generado con Ideogram:



Imagen generada con IA (Ideogram) ([CC BY-NC-SA <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>](https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es))

Prompt utilizado para generar la imagen: A powerful and colorful spray graffiti on a wall with the text “Stop cyberbullying”.

Rúbrica actividad 4.2 *Aplicar*

	Nivel 1	Nivel 2	Nivel 3
Claridad y relevancia de la información	La información presentada es clara, precisa y profundamente relevante para la prevención del ciberbullying. (2.5)	La información es adecuada pero podría ser más específica o relevante para la prevención del ciberbullying. (1.25)	No se presenta la infografía o no se incluye información sobre la prevención del ciberbullying. (0)
Creatividad y diseño visual	La infografía es visualmente atractiva y creativa, utilizando efectivamente iconos, imágenes y colores. (2.5)	La infografía es visualmente adecuada pero con un uso limitado de elementos creativos. (1.25)	No se presenta la infografía. (0)
Coherencia y estructura de los mensajes	Los mensajes son coherentes y bien estructurados, facilitando una comprensión clara y rápida de los contenidos. (2.5)	Los mensajes son algo coherentes pero la estructura podría mejorar para facilitar la comprensión. (1.25)	No se presenta la infografía o los mensajes son incoherentes. (0)
Reflexión sobre el proceso y efectividad de las recomendaciones	Reflexión detallada sobre el proceso de creación y justificación sólida de por qué las recomendaciones podrían ser efectivas. (2.5)	Reflexión presente pero superficial sobre el proceso y justificación básica de la potencial efectividad. (1.25)	No se incluye reflexión sobre el proceso ni justificación de la potencial efectividad. (0)

Módulo 4. Ciber escudos y secretos digitales

Otros formatos y autoría



Autoría

Título	Módulo 4 del curso "La Ciberseguridad en el ámbito educativo"
Descripción	<p>El módulo "Ciber escudos y secretos digitales" prepara a los participantes para implementar prácticas de protección avanzadas en sus entornos educativos digitales, asegurando tanto la conformidad con la LOPD como la protección efectiva de los menores en línea.</p> <p>Este módulo aborda la importancia de fomentar una cultura de seguridad digital, proporcionando herramientas y conocimientos para manejar y prevenir el ciberbullying, además de desarrollar una resiliencia digital en los docentes y estudiantes.</p>
Autor	Manuel Jesús Rivas Sández https://twitter.com/0xmrvs

Licencia	Creative Commons BY-NC-SA https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es	4.0
----------	--	-----



Versión imprimible PDF

Este material está diseñado para ser leído y trabajado de manera interactiva en un ordenador, pero si quieres puedes descargártelo en [este enlace](https://raw.githubusercontent.com/0xmrvias/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo4.pdf) [<https://raw.githubusercontent.com/0xmrvias/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo4.pdf>](https://raw.githubusercontent.com/0xmrvias/ciberseguridad-ambito-educativo-online/main/assets/PDF/modulo4.pdf) en formato pdf.

Obra publicada con Licencia Creative Commons Reconocimiento Compartir igual 4.0 <http://creativecommons.org/licenses/by-sa/4.0/>