1.5. PROTECCIÓN DE DATOS PERSONALES, PRIVACIDAD, SEGURIDAD Y BIENESTAR DIGITAL

Esta competencia hace referencia al desarrollo del compromiso docente que garantice el bienestar de la comunidad educativa a nivel digital.

- 1.5.0. Introducción.
- 1.5.1. Legislación sobre protección de datos personales, privacidad y garantías y derechos digitales en el ámbito educativo.
- 1.5.2. Seguridad en el acceso, almacenaje y recuperación de la información.
- 1.5.3. Ciberseguridad. Bienestar digital. Riesgos de la red.

Copyright 2026

Copyright 2026

1.5.0. Introducción.

Esta competencia se centra en la **protección de los datos personales, las comunicaciones y el acceso a los dispositivos**, dentro del ámbito educativo, para **evitar** los **riesgos** y **amenazas** que afecten a los **derechos** y **garantías digitales** de todos los miembros de la **comunidad educativa** contemplados en la **normativa vigente. Utilizar** de manera **responsable, segura** y **saludable** las tecnologías digitales para **evitar riesgos laborales, personales** y en el **entorno** y para garantizar el **bienestar físico, psicológico** y **social** del **alumnado** al utilizar las tecnologías digitales.

El **plan digital del centro** deberá recoger un conjunto de **medidas** que garanticen el **bienestar** de la **comunidad educativa.** Esta competencia está orientada al desarrollo del **compromiso docente** con este objetivo y se ejercita a través de cuatro **ejes:**

- la **protección** de **datos personales,** de la **privacidad** y de los **derechos digitales;**
- la **seguridad** en el acceso a los **dispositivos, sistemas** y **redes;**
- el **uso responsable** y **sostenible** de los recursos digitales desde el punto de vista **medioambiental** y
- las medidas orientadas a garantizar la **salud física** y **mental**

Un elemento fundamental para el desarrollo de esta competencia es la **protección de datos personales**, pues es una obligación que contrae todo docente en el desempeño de sus responsabilidades y su ejercicio está sujeto al deber de sigilo y debe ser completo desde un primer momento, por lo que no se puede graduar, en ningún caso, su aplicación.

La protección de datos se aplica **en todas las acciones docentes** en las que se debe realizar un tratamiento de datos personales - propios y de terceros (alumnado, familias, ...)- **de carácter administrativo**, para la **comunicación organizacional** y para el **desarrollo de actividades complementarias** a la enseñanza o el aprendizaje. Se concreta en la aplicación de las medidas y **protocolos de seguridad** en el centro, que deben desarrollar los establecidos por la legislación vigente. En función de la administración educativa para la que se trabaje o el centro concertado o privado en el que desempeñe la docencia, estos protocolos pueden cambiar, aunque siempre van a exigir la aplicación de unos elementos comunes.

El desarrollo de esta competencia en el tratamiento de datos personales de carácter administrativo se complementa con el ejercicio **responsable** del **tratamiento de datos** en los procesos de **enseñanza, aprendizaje** y **evaluación** que tienen su correspondencia en las áreas 2, 3, 4 y 5. Conviene resaltar que no se incluirían las medidas orientadas a la formación del alumnado en este

Copyright 2026

tema, puesto que ya están incluidas en el área 6.

Los **contenidos** que integran esta competencia son:

- **Legislación** sobre **protección** de **datos personales, privacidad** y **garantías** y **derechos digitales** en el ámbito educativo.
- **Seguridad** en el **acceso, almacenaje** y **recuperación** de la información.
- **Bienestar digital** y **uso responsable, saludable** y **sostenible** de los recursos digitales.

Según el MRCDD un docente con nivel B2 en esta competencia...	
1.5.B2.1	Colabora en el **diseño** y la **evaluación** de los **protocolos** para la aplicación de las **medidas** establecidas por la A. E. o los titulares del centro sobre **protección de datos personales** y **garantías de derechos digitales** de acuerdo con la normativa vigente.
1.5.B2.2	Contribuye al **diseño** del **plan de convivencia** en lo relativo al **uso de las tecnologías** digitales y a su impacto en el **bienestar físico y psicológico** del alumnado.
1.5.B2.3	Colabora en la **inclusión**, en el plan digital de centro, de **actuaciones** que promuevan la **sostenibilidad medioambiental** en el uso de los recursos digitales y su posterior seguimiento.
1.5.B2.4	**Ayuda**, de manera informal, a otros docentes de su centro en la **aplicación de las medidas** sobre **protección de datos personales**.

Copyright 2026

1.5.1. Legislación sobre protección de datos personales, privacidad y garantías y derechos digitales en el ámbito educativo.

¿A qué nos referimos cuando hablamos de "**tratamiento de datos**"? Es cualquier **operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales**, ya sea por procedimientos automatizados o no, como la **recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión** o cualquier otra forma de habilitación de **acceso, cotejo** o **interconexión, limitación, supresión** o **destrucción.**

Copyright 2026



Imagen: Agencia Española de Protección de Datos. https://www.aepd.es/es/node/47545

En **España,** la legislación sobre protección de datos personales en el ámbito educativo se rige por la **Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales** (**LOPDGDD**) y el **Reglamento General de Protección de Datos** (**RGPD**) de la **Unión Europea.**

La **LOPDGDD** establece la **obligación de proteger los datos personales del alumnado y el profesorado**, asegurando su **confidencialidad e integridad,** y establece un **sistema de control de acceso a los datos** por parte de terceros. Además, la ley establece los **derechos ARCO (acceso, rectificación, cancelación y oposición**) que pueden ejercer los titulares de los datos.

Por otro lado, en cuanto a la **privacidad y garantías digitales**, la ley establece la obligación de **proteger los derechos de propiedad intelectual** e industrial en el ámbito educativo y **garantizar** la **privacidad de los documentos**, el **correo electrónico** y la **información comunicada a través de medios digitales**. También se deben establecer **medidas de seguridad** para prevenir posibles ataques informáticos.

Copyright 2026

En cuanto a los **derechos digitales**, la **LOPDGDD** establece la **protección de los derechos de los usuarios** en el entorno digital, incluyendo el **derecho al acceso universal a la conectividad y a la información**, la **neutralidad** de la red y la **seguridad digital**.

Desde la tramitación de los procesos de **admisión del alumnado**, los centros educativos tratan **información personal** del **alumno** para proporcionarle los **servicios** de **educación** y **orientación,** todo ello con finalidades tan distintas como la confección de los expedientes académicos, la gestión del servicio de comedor y transporte escolares, la concesión de ayudas, la concesión de premios académicos, la organización y promoción de actividades educativas, culturales, deportivas y de ocio, la evaluación académica, la orientación del alumnado con necesidades educativas especiales o específicas, la corrección disciplinaria.

Por lo que se recogen y registran **múltiples datos personales,** se captan y difunden **imágenes** del alumnado y profesorado, se organizan eventos, se utilizan recursos didácticos digitales, se comunican datos a diversas instituciones...

Todo ello implica el **tratamiento de un considerable volumen de datos personales** que afectan a toda la comunidad educativa.

https://www.youtube.com/embed/ZICN29pU-cc

Copyright 2026



Imagen: Agencia Española de Protección de Datos. https://www.aepd.es/es/documento/quien-es-quien-centros-docentes.pdf

> ¿A qué nos referimos cuando hablamos de **"seguridad y privacidad en Internet**"? Nos referimos a la **protección** de **datos personales,** la **confidencialidad** de la información y la salvaguardia de la **integridad** de las **comunicaciones** en el entorno digital. A las **medidas** y **prácticas** utilizadas para **proteger** la **información** y los sistemas en línea de posibles amenazas como malware, hacking, robo de datos, phishing, entre otros. Implica la implementación de contraseñas seguras, antivirus, firewalls, actualizaciones de software y el uso de conexiones seguras.

El uso de las tecnologías digitales es diario y continuado, por ello, desde la perspectiva de la **seguridad de la información,** hemos de extremar las precauciones pues gestionamos información de manera directa y somos, en muchas ocasiones, el **primer eslabón** de la cadena de **seguridad** de los datos manejados.

Copyright 2026

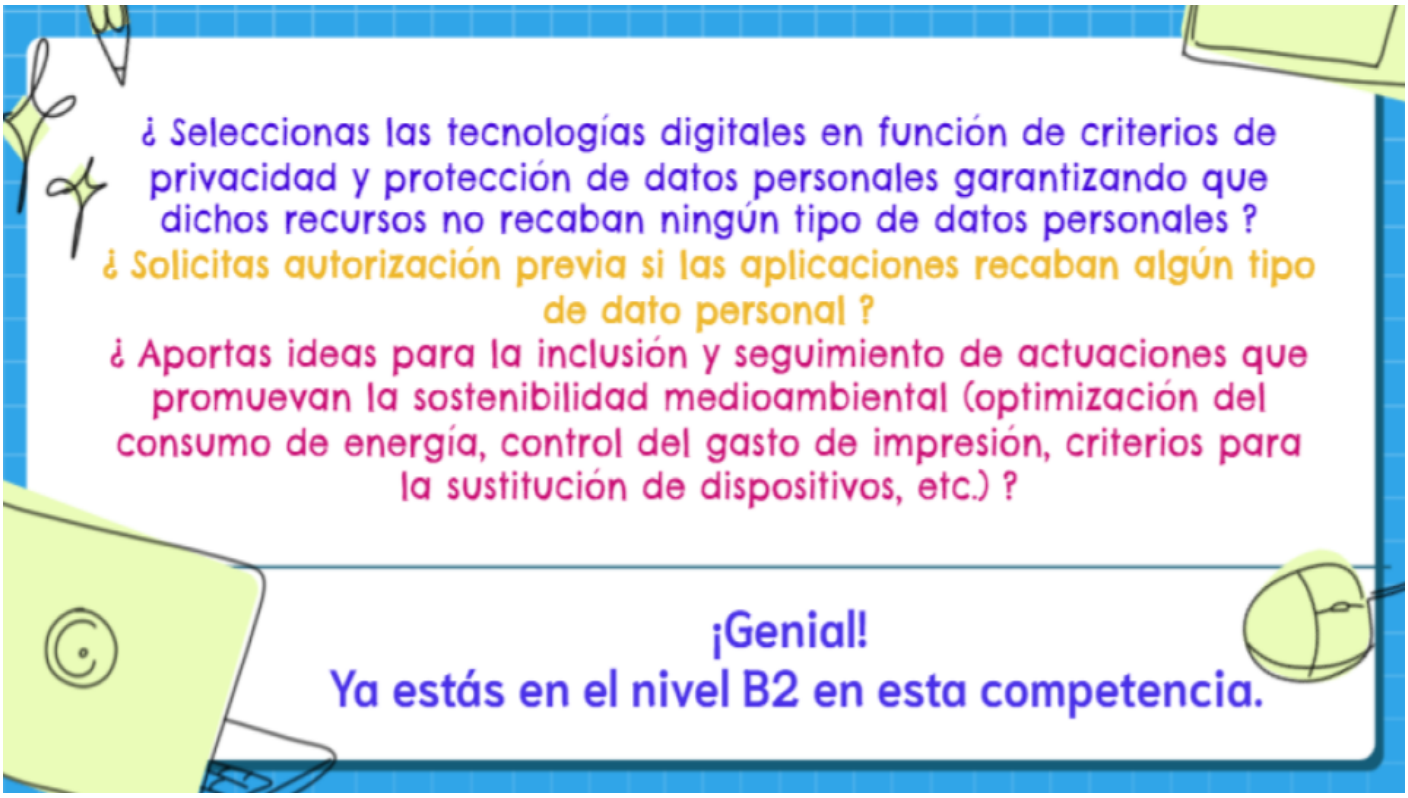
Este es **el Decálogo** que nos recomienda seguir el medio técnico del Gobierno de Aragón, **Aragonesa de Servicios Telemáticos**:



Imagen: Aragonesa de Servicios Telemáticos. https://ast.aragon.es/actualidad/decalogo-de-seguridad

El INCIBE (Instituto Nacional de Ciberseguridad) pone a nuestra disposición unos recursos valiosísimos para ayudarnos a comprender bien y tomas medidas adecuadas para mejorar la privacidad. En su sección "Privacidad, identidad digital y reputación on line" encontramos muchos materiales para ello.

Copyright 2026



Copyright 2026

1.5.2. Seguridad en el acceso, almacenaje y recuperación de la información.

La transformación digital ha llevado a que tanto el alumnado como el profesorado, tenga acceso a una gran cantidad de información en línea. Esto les facilita el acceso a materiales de estudio y herramientas educativas. Sin embargo, el acceso a información digital también implica algunos riesgos. La gestión de la seguridad en el acceso digital y el almacenamiento de información en el ámbito educativo, resulta fundamental para garantizar la privacidad de los datos.

> Para **garantizar la seguridad digital**, se requiere la implementación de medidas de seguridad como el **uso de contraseñas seguras**, la **autenticación de usuarios**, la **validación de acceso** y la **actualización continua de sistemas operativos y aplicaciones** utilizadas.

Por otro lado, el **almacenamiento digital** de información es clave para la **organización de contenidos**, el **trabajo colaborativo** y para la realización de **copias de seguridad** que permitan evitar la pérdida de información en caso de fallos de dispositivos o ataques cibernéticos. Para ello, pueden utilizarse herramientas de **almacenamiento en la nube** tanto gratuitas como de pago. Estas herramientas permiten acceder a la información desde múltiples dispositivos y en diferentes ubicaciones, siempre y cuando se garantice la seguridad de acceso a ellos.

La **recuperación de la información** se refiere a la capacidad de **restaurar** los datos que se han perdido en los dispositivos digitales. Aunque los sistemas de almacenamiento en la nube son una herramienta muy útil, también conllevan riesgos de pérdida de datos. Para minimizar estos riesgos, se debe hacer una copia de seguridad de los materiales más valiosos y guardarlos tanto en **dispositivos físicos** como en servicios de **almacenamiento en línea.**

Copyright 2026

La **gestión de la seguridad digital** es una tarea cada vez más importante en el ámbito educativo. La necesidad de garantizar el **acceso seguro a la información**, **proteger la privacidad** y **recuperar la información** son elementos fundamentales para lograr un entorno educativo tranquilo y eficiente en el uso de las nuevas tecnologías. Por ello, la formación y la conciencia sobre estas cuestiones son cada vez más importantes en el ámbito de la educación.

Medidas de seguridad pasiva

Las medidas de seguridad pasiva son aquellas que **se aplican de forma permanente** y están diseñadas para **minimizar el riesgo de acceso, almacenamiento y recuperación de información en la red**.
Algunas **medidas** de seguridad pasiva son:

- **Control de acceso**: limitar el acceso a la información sensible o confidencial a las personas autorizadas mediante la utilización de contraseñas, autenticación de dos factores, control de acceso físico, etc.
- **Encriptación**: utilizar sistemas de encriptación para proteger la información durante su almacenamiento y transmisión.
- **Copias de seguridad**: realizar copias de seguridad regulares para evitar la pérdida de datos en caso de algún accidente con ellos.
- **Firewall**: utilizar firewall para proteger la red de accesos no autorizados.
- **Actualización y parches**: mantener actualizado el software y aplicar parches de seguridad para evitar vulnerabilidades.
- **Monitoreo y detección**: monitorear la red para detectar y prevenir posible ataques cibernéticos.
- **Capacitación de usuarios**: concienciar y capacitar a los usuarios sobre las buenas prácticas de seguridad en la red para evitar incidentes.

Medidas de seguridad activa

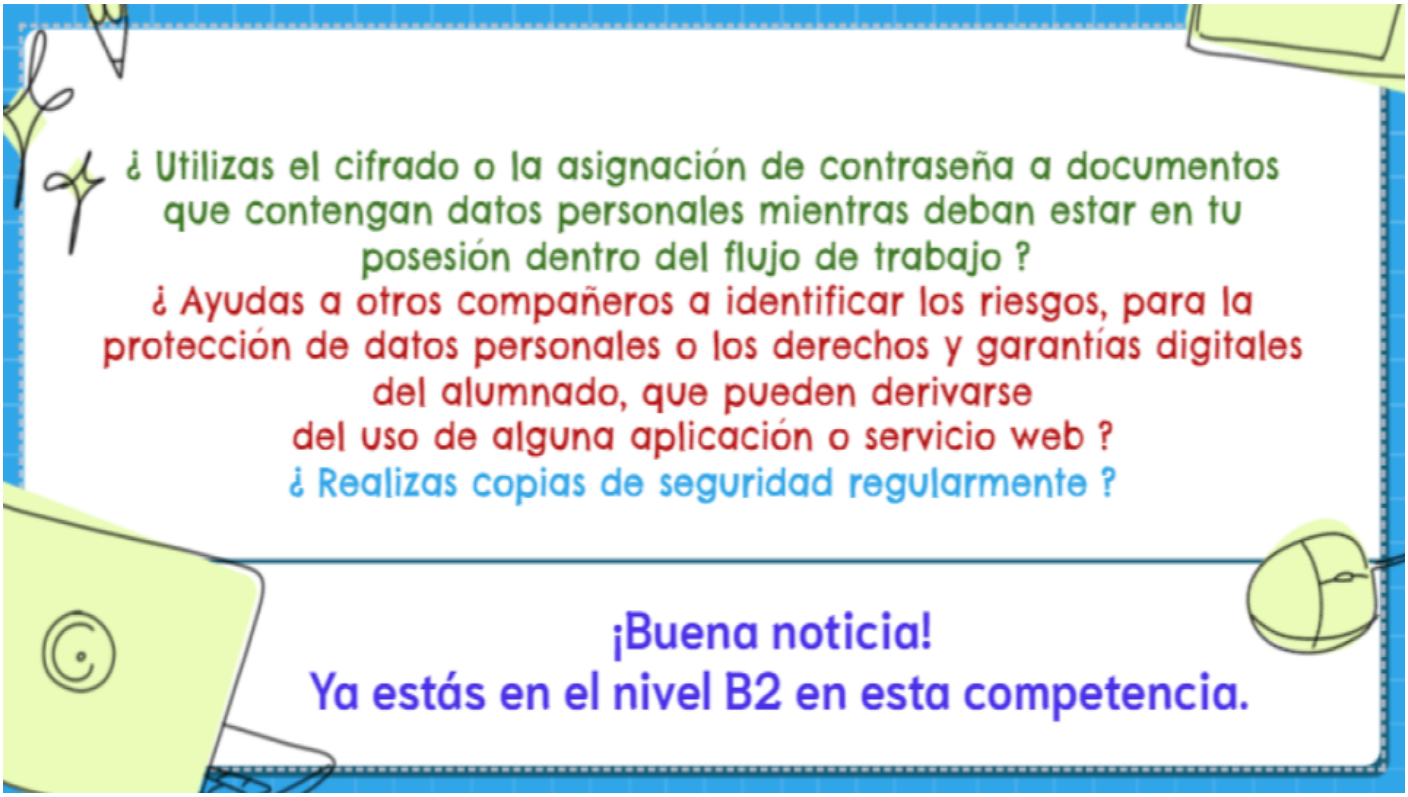
Las medidas de seguridad activa son aquellas que **se aplican en tiempo real** y se utilizan para **detectar y responder rápidamente ante un incidente de seguridad en la red**.
Algunas **medidas** de seguridad activa son:

- **Software antivirus y malware**: utilizar un software específico que detecte y bloquee software malintencionado, virus y programas espía.
- **Firewall**: utilizar un firewall como medida no solo de seguridad pasiva sino también activa para controlar el tráfico de la red y evitar instrusiones.
- **Detección de intrusos (IDS/IPS)**: configurar sistemas de detección de intrusos y prevención de intrusiones que alerten en caso de una actividad sospechosa en la red.
- **Análisis de vulnerabilidades**: realizar análisis periódicos para detectar y corregir vulnerabilidades en la red.
- **Monitoreo de la actividad de los usuarios**: supervisar la actividad de los usuarios de la red para detectar comportamientos inusuales o sospechosos.
- **Configuración de políticas de seguridad**: establecer políticas y directrices de seguridad clara que ayuden a asegurar que todos los usuarios de la red cumplan con las normas establecidas.
- **Respuesta a incidentes**: tener un plan de respuesta de seguridad en caso de un incidente de seguridad en la red, para minimizar su impacto y recueprar la información perdida o dañada.

Copyright 2026

Es necesario tomar conciencia de todas estas medidas y aplicar todas aquellas que estén a nuestro alcance:

- Utilizar el **almacenamiento** en la **nube** y también realizar copias de seguridad **físicas** de los documentos importantes.
- Establecer un **calendario** de realización de **copias** de **seguridad** periódico.
- Utilizar **contraseñas** de acceso para los documentos que contengan información sensible. En ocasiones, confiamos en que la información está contenida en una unidad a la que sólo tenemos acceso nosotros, pero cabe la posibilidad, incluso, de extraviarla.
- Instalación de **antivirus** y **actualización** del mismo.
- Uso de **herramientas** y **aplicaciones** seguras y **actualización** de las mismas.
- Evitar compartir documentos de la nube que contengan datos personales para cualquier usuario que tenga el enlace, sino utilizar la opción de **acceso restringido.**



1.5.3. Ciberseguridad. Bienestar digital. Riesgos de la red.

Ciberseguridad

> ¿A qué nos referimos cuando hablamos de **ciberseguridad?** Nos referimos a las **medidas** y prácticas utilizadas para **proteger** los **sistemas informáticos, redes** y **datos** de posibles amenazas o ataques cibernéticos. Incluye la **protección de la información confidencial**, la **prevención de accesos no autorizados**, la **detección de actividades maliciosas** y la **respuesta ante incidentes de seguridad**. La ciberseguridad abarca tanto a nivel personal, en la protección de nuestros dispositivos y datos personales, como a nivel empresarial, donde se busca salvaguardar la información de la organización y proteger su infraestructura tecnológica.

En la página del **INCIBE (Instituto Nacional de Ciberseguridad)** podemos encontrar mucha **ayuda** con respecto a estas cuestiones. Resulta prácticamente imposible decantarse por una u otra guía, pues todas son muy interesantes y necesarias. Puedes elegir aquella que consideres más necesaria o de mayor interés para ti en este momento o ir leyendo todas poco a poco. También encontrarás muchos recursos para trabajar con tu alumnado (fichas, talleres, recursos descargables, actividades interactivas, test de autoevaluación).

	En esta guía del INCIBE encontramos las claves para respaldar fácilmente la información almacenada en dispositivos Windows, Mac, Android e iOS.



En estas fichas del INCIBE encontramos información sobre las características de los navegadores más utilizados, especialmente las relacionadas con aspectos de privacidad y seguridad.



Esta guía de ciberseguridad del INCIBE está pensada para los más mayores, pero es muy completa e interesante, así que, si encuentras tiempo y tienes interés en ampliar y afianzar tus conocimientos al respecto: te recomendamos su lectura.

Copyright 2026



Esta guía del INCIBE está formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet así como las medidas de protección que debemos aplicar para evitarlos.



En este recurso se nos muestran tres situaciones típicas con las que cualquier usuario de una red social se ha encontrado una vez. Se trata de seguir el árbol de decisiones para tomar siempre el camino correcto y navegar seguro por las redes sociales.



Es una aplicación gratuita que ayuda a proteger el dispositivo móvil Android. Permite conocer el estado de seguridad del dispositivo, mostrando soluciones a posibles riesgos a los que esté expuesto y proporcionando algunos consejos que ayudarán a mejorar su seguridad.

Copyright 2026

Bienestar digital

> ¿A qué nos referimos cuando hablamos de **bienestar digital**? El bienestar digital se refiere al **estado de equilibrio y bienestar** de las personas **en relación con su uso de la tecnología digital**.

El bienestar digital implica adoptar **hábitos y prácticas saludables** en relación con la **tecnología,** como establecer **límites** en el tiempo de uso, **desconectarse** regularmente, tener **períodos de descanso** adecuados, **evitar la adicción** a los dispositivos y **promover** un **uso responsable** de la tecnología.

Además, el bienestar digital también se refiere a la **capacidad** de utilizar la tecnología de manera **productiva** y **positiva,** como utilizarla para el **aprendizaje,** el **crecimiento personal,** la **comunicación** y el **desarrollo de habilidades.** También implica la búsqueda de un **equilibrio** entre el uso de la tecnología y otras actividades importantes en la vida cotidiana, como el trabajo, el tiempo en familia, el ejercicio físico y el tiempo al aire libre. En definitiva, **se trata de utilizar la tecnología de manera consciente y equilibrada, para que beneficie a nuestra salud y calidad de vida, en lugar de perjudicarla.**

Cómo mejorar el bienestar digital

> Prestar atención a los siguientes aspectos puede ayudarnos a **mejorar nuestro bienestar digital:**

- **Límites de tiempo de exposición a las pantallas**: Es importante establecer límites y horarios para el uso de dispositivos digitales. Esto evitará la sobreexposición y nos permitirá dedicar tiempo a otras actividades importantes.

https://www.youtube.com/embed/f0_2XBod8Hg

- **Gestión del tiempo**: Organizar y administrar nuestro tiempo en línea de manera eficiente es fundamental. Establecer una agenda y priorizar las tareas ayudará a evitar la sensación de estar siempre conectados.
- **Privacidad y seguridad en línea**: Mantener nuestros datos personales seguros y protegidos es esencial. Utilizar contraseñas fuertes, evitar compartir información sensible y revisar regularmente las configuraciones de privacidad en las redes sociales son algunas medidas que podemos tomar.

Copyright 2026

https://www.youtube.com/embed/4YSGMBv56Ec

- **Desconexión:** Es importante permitirnos momentos de desconexión digital. Esto puede incluir períodos de tiempo sin dispositivos electrónicos, como apagar el teléfono durante la noche o los fines de semana.

https://www.youtube.com/embed/3jEosMJEyK4

- **Socialización equilibrada**: Las relaciones sociales digitales son importantes, pero también debemos fomentar los encuentros en persona y la comunicación cara a cara. Encontrar equilibrio entre nuestras interacciones en línea y fuera de línea es esencial para nuestro bienestar.

https://www.youtube.com/embed/eo14JAmkvs4

- **Control de la información consumida**: Es crucial ser selectivos con la información que consumimos en línea. Elegir fuentes confiables, evitar la sobreexposición a noticias negativas y mantener una actitud crítica hacia la información que encontramos ayudará a mantener una perspectiva saludable.
- **Cuidado de nuestra salud física**: El uso prolongado de dispositivos digitales puede tener un impacto en nuestra salud física. Es importante cuidar nuestra postura, hacer pausas regulares para levantarnos y estirarnos, y mantener una rutina de ejercicio físico.

https://www.youtube.com/embed/wJHbD6CGQDs

- **Autoevaluación:** Regularmente debemos evaluar cómo nos sentimos en relación con nuestro uso de dispositivos digitales. Si sentimos que estamos haciendo un uso excesivo o que nuestra relación con la tecnología es negativa, es importante buscar apoyo y ayuda profesional si es necesario.

Riesgos de la red

¿Aquénosreferimoscuandohablamosde" **riesgosdela red**"? Nos referimos a los **peligros** o **amenazas** que pueden surgir al **utilizar Internet** y las **tecnologías digitales** en el ámbito educativo.

Estos riesgos pueden afectar tanto a **docentes** como a **estudiantes** y pueden incluir:

- **Contenido inapropiado**: Acceder a información, imágenes o videos que sean inapropiados para la edad y el nivel de madurez de los estudiantes.

https://www.youtube.com/embed/5HWBDPW3xbQ

- **Ciberacoso:** Ser víctima de intimidación, humillación o acoso a través de las redes sociales, mensajes de texto u otras plataformas en línea.

https://www.youtube.com/embed/G8iciqvXnmk

- **Robo de identidad**: Que alguien pueda utilizar de manera fraudulenta los datos personales o contraseñas de los estudiantes o docentes.
- **Engaños y estafas**: Ser víctima de fraudes en línea, donde se solicitan datos personales, o se realizan compras falsas, entre otros.
- **Adicción a internet y las redes sociales**: Desarrollar una dependencia excesiva o compulsiva hacia las tecnologías y las redes sociales, lo que puede afectar el rendimiento académico y la salud mental de los estudiantes.

https://www.youtube.com/embed/lyOoHtyyI0U

https://www.youtube.com/embed/Gh2LJGQc9t8

- **Falta de privacidad**: Compartir demasiada información personal en línea, sin tener en cuenta los riesgos de que sea utilizada de manera indebida.

Copyright 2026

https://www.youtube.com/embed/SiqpwmTpb68

- **Violencia en línea**: Exponerse a contenidos violentos, como imágenes de agresiones físicas, incitación al terrorismo o juegos que promueven la violencia.
- **Falsificación de identidad**: Suplantar la identidad de otra persona, haciéndose pasar por ella en internet.

https://www.youtube.com/embed/i_92-NovRT0

> Es importante que estudiantes y docentes estén conscientes de estos riesgos y tomen medidas para protegerse a sí mismos y a los demás mientras usan internet y las TIC en el contexto educativo.

Podríamos agrupar estos **riesgos** en torno a:

1. Acceso a **contenido no apropiado** para menores.
2. **Ciberacoso.**
3. **Adicción** a las redes sociales.
4. **Riesgos de seguridad informática**: las redes y los dispositivos móviles son vulnerables a los ataques cibernéticos como la suplantación de identidad, la interceptación de comunicaciones, las amenazas de malware y la exposición de información personal.
5. **Falta de control parental**.

> Es importante que se implementen medidas preventivas y de seguridad en el ámbito educativo para hacer frente a estos riesgos y garantizar un entorno de aprendizaje seguro y saludable para los estudiantes.

Ciberseguridad en el puesto de trabajo

Compartimos este documento sobre **ciberseguridad en el puesto de trabajo** elaborado por **Eloy Villa,** experto en ciberseguridad, como resumen del asesoramiento realizado a docentes en el marco de una actividad para la formación del profesorado en este ámbito.

GUÍA - RESUMEN
CIBERSEGURIDAD EN EL PUESTO DE TRABAJO

Material de la sesión formativa asociada a la actividad nº 9506 (DOCEO) realizada con el personal del Equipo de Orientación Educativa de Atención Temprana

CONTRASEÑAS

- ☐ Usar una contraseña fuerte (8-10 caracteres, con MAYUSCULAS, minúsculas, números y símbolos especiales, como . , - $ % & ( ) @#)
- ☐ No usar la misma contraseña para todo
- ☐ Se puede pensar en usar un patrón, como por ejemplo, una palabra, con las vocales en minúsculas, las consonantes en mayúsculas, un año partido en 2 partes y un símbolo especial, añadiendo una 't' para Twitter, una 'f' para Facebook, una 'g' para Gmail, …
- ☐ Por ejemplo: 20eJea23#.t para Twitter, 20eJea23#.f para Facebook, etc.
- ☐ No dejar las contraseñas a la vista (post-its, apuntes, fichero con contraseñas en el escritorio, …

CORREO ELECTRÓNICO

- ☐ Prestar atención al dominio de donde viene un correo (Ej. En juan@gmail.com el dominio es Gmail.com, que es conocido y fiable). Si no se ve, desplegar la cabecera para ver más detalles
- ☐ Especial atención a los enlaces que vienen dentro del correo. Si se pone el ratón sobre ellos sin hacer click, aparece un rectángulo gris con la información real del enlace a donde nos lleva.
- ☐ Cuidado con los ficheros adjuntos. Revisar si son docx (documentos Word), pdf (se abren con el Adobe Reader), xls (ficheros Excel), jpg (imágenes), … aunque hay muchos más. Revisar qué es antes de abrirlos.
- ☐ Si nos solicitan datos bancarios, privados o sensibles, podemos hacer la comprobación por teléfono antes de mandarlos, llamando a la persona que nos lo solicita por teléfono y confirmar que realmente es esa persona la interesada.
- ☐ Las tildes mal escritas pueden ayudar a identificar correos maliciosos.
- ☐ Si algo se sale de lo normal, sospechar siempre.
- ☐ Se puede ampliar más información en la web oficial de Microsoft, visionando unos vídeos muy cortitos en esta dirección:

https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

COPIAS DE SEGURIDAD

- ☐ Regla del 3-2-1: mantener 3 copias "vivas". Al hacer la 4ª se puede eliminar la más antigua. En 2 dispositivos distintos (2 pendrives diferentes y en diferentes lugares). 1 vez por semana (recomendable)
- ☐ Las políticas de la copia de seguridad pueden variar dependiendo de la carga de trabajo (si se hace mucha documentación un día puede ser interesante hacer una copia ese día sin esperar al día programado.

CLOUD / NUBE

- ☐ Se puede hacer uso de la nube para mantener copias de seguridad en One Drive o Google Drive
- ☐ Los programas agentes sincronizadores pueden ser útiles, pero personalmente, prefiero subir manualmente los documentos a la nube.
- ☐ Tener en cuenta que lo que se sube a la nube si está compartido, se hace público. Compartir sólo lo que sea necesario, y si se comparte una carpeta completa, asegurarse de que en dicha carpeta no se sube material personal o sensible.

TELÉFONOS MÓVILES

- ☐ Eliminar todas las wifis que no se necesiten tener almacenadas
- ☐ Instalar un programa antivirus como ESET o CONAN MOBILE
- ☐ Revisar los permisos que otorgamos a las aplicaciones al instalarlas. CONAN MOBILE puede ayudarnos con esto.
- ☐ Mantenerlo actualizado, tanto el propio sistema Android como las aplicaciones

- ☐ Decidir si es necesario o no tener activos los asistentes de voz, como Siri, Alexa, Cortana, Ok Google, …

CIFRADO

- ☐ Cifrar con la utilidad en Android la memoria del teléfono (en ajustes -> almacenamiento -> cifrado de memoria) (la ruta puede variar según dispositivos)
- ☐ Si en Windows no aparece en cifrado de BitLocker, puede que sea que no está disponible para la versión Home de Windows. Podemos activarlo siguiendo estos pasos de la web de Microsoft:

https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_10

o en la versión de Windows 11:

https://support.microsoft.com/es-es/windows/activar-el-cifrado-de-dispositivo-0c453637-bc88-5f74-5105-741561aae838#ID0EBD=Windows_11

- ☐ Sería importante cifrar los pendrives que vayan a salir de la oficina, por si se pierden, que quien los encuentre no pueda acceder a la información del mismo.

PUESTO DE TRABAJO

- ☐ Mantener el puesto de trabajo con la mínima información sensible expuesta (informes, documentos, post-its, …) para evitar que posibles visitas o trabajadores ajenos al departamento accedan a dicha información.
- ☐ Si tenemos que irnos de nuestro puesto de trabajo, podemos bloquear la sesión pulsando las teclas



(Recordad el ataque David Hasselhoff con los Perritos)

NAVEGADOR DE INTERNET

- ☐ Revisar la ruta de las webs que estemos visitando.
- ☐ Recordar que el candadito verde no quiere decir que la web sea buena, si no que la comunicación es cifrada, sólo eso
- ☐ Si la web que estamos visitando no tiene el certificado correcto (es http en vez de https o tiene el certificado caducado), es un riesgo seguir navegando en dicha web.
- ☐ Podemos trabajar en “modo incógnito”, abriendo Google Chrome y pulsando las teclas



El modo incógnito no nos protege de nada, sólo nos hace no cargar cookies, ni historial de navegación, ni historial de búsquedas. Puede no ser útil si tenemos que volver a trabajar en ese equipo, pero tenemos la privacidad de que si la siguiente persona que use el equipo no es de confianza no tendrá esa información privada nuestra.

- ☐ Recordad cerrar sesión siempre que ya no necesitéis tener acceso a la web que sea, más aún si no es en nuestro equipo donde la hemos abierto.

Copyright 2026

Imagen: Eloy Villa, experto en ciberseguridad (informaticaeloy.com). CC-BY-NC-SA.

