6.4. Uso responsable y bienestar digital

- 6.4.0. Introducción
- 6.4.1. Uso responsable
- 6.4.2. Reciclaje de dispostivos
- 6.4.3. Ejemplos de aplicación

Copyright 2026

6.4.0. Introducción

Esta competencia se despliega a la hora de **conocer, diseñar y aplicar estrategias pedagógicas para que el alumnado desarrolle un grado de competencia que le permita realizar un uso seguro y responsable de las tecnologías digitales.** El elemento común de la competencia que el alumnado ha de desarrollar es la protección y la seguridad, pero deberá aplicarse en distintos ámbitos: los dispositivos, los datos personales y la privacidad, tanto propia como ajena, la salud física y mental y el medio ambiente y la sociedad. Esto **implica que el alumnado**:

- Conozca los riesgos y beneficios, tanto personales como sociales y medioambientales, que puede comportar el uso de las tecnologías digitales.
- Adopte hábitos de uso saludable, ecológico y sostenible, que incorporen de forma sistemática la aplicación de medidas de seguridad para proteger sus dispositivos, datos personales, privacidad y contenidos.
- Tome decisiones y haga un uso y consumo responsable de las tecnologías digitales y sepa actuar de forma adecuada frente a los problemas que puedan surgir y afecten a la seguridad o al bienestar físico o psicológico propio o de otras personas.

> Esta competencia está vinculada con la 1.5. Protección de datos personales, privacidad, seguridad y bienestar digital, pero presenta notables diferencias con respecto a ella, ya que la competencia 6.4. Uso responsable y bienestar digital tiene un carácter eminentemente pedagógico, mientras que la 1.5. requiere que el profesorado sea competente en la adopción de medidas de seguridad y de protección de datos personales y privacidad en el ejercicio de todas las funciones que tiene encomendadas, así como desarrollar medidas proactivas para procurar el bienestar físico, psicológico, social y emocional del alumnado en los entornos digitales. Estas últimas acciones estarían relacionadas con la convivencia positiva en el centro educativo.

Los **contenidos** necesarios para el desarrollo de esta competencia docente son:

- Estrategias pedagógicas para el desarrollo de la competencia digital del alumnado.
- Técnicas para la protección de dispositivos (ordenadores, tabletas, teléfonos inteligentes, asistentes personales, electrodomésticos y vehículos gestionados por IoT, tecnologías portables y de mobiliario urbano), los datos personales y la privacidad.
- Las tecnologías digitales y la salud. Prácticas saludables a la hora de utilizar las tecnologías digitales.

Copyright 2026

- Riesgos y beneficios de las tecnologías digitales. Protección de datos personales y privacidad.
- Tecnologías digitales, justicia social, protección del medioambiente y sostenibilidad.
- Normativa sobre protección de datos personales y garantía de los derechos digitales.

El desempeño establecido para el B2 implica el "*Diseño y adaptación de las estrategias pedagógicas para potenciar el desarrollo de la competencia digital del alumnado en el uso responsable, seguro, crítico, saludable y sostenible de las tecnologías digitales*" *al comprobar si:*

- *6.4.B2.1. Diseña o adapta nuevas propuestas pedagógicas, a partir de la reflexión y evaluación de su propia práctica, para que el alumnado desarrolle su competencia a la hora de emplear las tecnologías digitales de forma responsable, segura, crítica, saludable y sostenible*

Esto es, se trata de ver si diseño o adapto distintas propuestas didácticas para integrar en los procesos de enseñanza y aprendizaje el desarrollo de la competencia del alumnado para utilizar de forma responsable, segura, crítica, saludable y sostenible las tecnologías digitales. **Ejemplos**:

- A partir de la pregunta “¿Qué es RoHS?”, pido a mi alumnado que realice una auditoría de los dispositivos digitales que emplean de forma habitual.
- Sugiero al alumnado realizar un vídeo instructivo con recomendaciones sobre hábitos ergonómicos y rutinas de descanso ocular al usar dispositivos y pantallas y, posteriormente, crear un código QR con enlace al vídeo para que otros escolares puedan consultarlo en el rincón, espacio o aula digital.
- Propongo a mi alumnado, en un proyecto interdisciplinar de Economía, Matemáticas, Tecnología, y Valores Cívicos y Éticos, que analice los datos que debería recabar y enviar a la empresa un robot doméstico para el barrido de suelos, elabore un programa para su tratamiento con el fin de hacer mejoras en el diseño de un nuevo modelo y elaborar el folleto de instrucciones e información sobre protección de datos que se debe facilitar al consumidor
- Utilizo el poema “A una nariz” en mi clase de Literatura, como base para tratar el tema de los trolls y el flaming en las redes sociales, establecer cuál debería ser la respuesta óptima en estos casos, analizar los tipos de acoso más habituales y crear un soneto que recoja las conclusiones.
- Planteo a mi alumnado la búsqueda e identificación en Internet de ofertas de empleo y negocios e inversiones fraudulentos en los que se aplica el principio de la pirámide de Ponzi -potenciado por la enorme capacidad de alcance de las herramientas digitales para, posteriormente, elegir una de ellas y hacer una exposición sobre el procedimiento que siguen y los factores psicológicos que caracterizan tanto al timador como a la víctima.

Copyright 2026

6.4.1. Uso responsable

Es importante hacer un uso responsable de los dispositivos digitales y seguir unas **pautas saludables** al utilizar las nuevas tecnologías para preservar el bienestar a nivel físico, psicológico y social. Utilizarlos de forma segura supone ser consciente de los riesgos que conlleva navegar en un entorno virtual, reflexionar e intentar poner de tu parte para reducir el impacto que la "**basura**" **tecnológica** ejerce sobre el medio ambiente y sobre la salud. En estos dos apartados (6.3.1. y 6.3.2.) trataremos de dar respuesta al indicador de esta competencia.

> 6.4.B2.1. Diseña o adapta nuevas propuestas pedagógicas, a partir de la reflexión y evaluación de su propia práctica, para que el alumnado desarrolle su competencia a la hora de emplear las tecnologías digitales de forma responsable, segura, crítica, saludable y sostenible

En este punto, se darán algunas de las claves que te indicarán como hacer un uso responsable de los dispositivos, de modo que te permitan relacionarte de forma saludable con el mundo digital. Algunas de ellas son establecer tiempos de uso o tener en cuenta la ergonomía.

¿A qué llamamos bienestar digital?

Se denomina bienestar digital al estado que se alcanza cuando se consigue establecer una relación saludable con la tecnología digital, aprovechando su potencial para lograr **objetivos** de manera que no interrumpa, interfiera o se interponga en la actividad cotidiana.

¿Qué ventajas nos ofrece un entorno digital?

- **Autoaprendizaje:** permite aprender de forma individual a lo largo del tiempo, por investigación, descubrimiento o prueba y error.
- **Trabajo colaborativo:** puesto que puedes planificar actividades que te permitan cooperar en grupo para alcanzar un mismo objetivo.
- Transformar el proceso de **búsqueda de** información **en Internet en aprendizaje significativo,** lo cual requiere de una selección previa o filtrado, evaluación objetiva de su calidad, procesamiento de los datos e interpretación de la información que has localizado.
- Permite la **exposición, expresión y comunicación** de contenidos o aprendizajes adquiridos, haciendo uso de diferentes herramientas digitales, potenciando la creatividad y haciendo uso de narrativas digitales.

Copyright 2026

- Da la oportunidad de **aprender a relacionarse adecuadamente** con los **dispositivos digitales** manteniendo hábitos saludables y protegiéndolos de los potenciales peligros que existen cuando los conectamos a la red.

¿Qué hábitos debo establecer para lograr una situación de bienestar digital?

- **Pautas de actuación**
  - Establecer **horarios y tiempos de uso** de los dispositivos digitales que sean flexibles, pero basados en criterios realistas y fundamentados. Es interesante utilizar algunas de las herramientas que incluyen actualmente los sistemas operativos como **Android**, en las que haciendo uso de un gráfico circular se muestra el tiempo que hemos pasado en cada una de las aplicaciones a lo largo del día mediante diferentes colores.
  - Utilizarlos de forma equilibrada y nunca de un **modo obsesivo**, evitando provocar problemas de aislamiento y de adicciones en su vida adulta. Cuando se trata de un menor, es conveniente colocar el ordenador en **zonas comunes** del hogar para favorecer que los adultos puedan detectar más fácilmente la exposición a los riesgos que conlleva su conexión a Internet.
  - El papel de las familias es muy relevante, pues es parte de su responsabilidad **regular el tiempo** que los menores dedican a cada actividad:
    - tareas escolares
    - ocio
    - relaciones sociales *online*
    - interacción social presencial, etc.

El **vídeo** titulado ***Prevención del uso excesivo en Internet***, puede servirte a modo de orientación:

https://www.youtube.com/embed/1ln9lnTYsvs

YouTube / is4k. *Prevención del uso excesivo en Internet* (Licencia de YouTube estándar)

El **Instituto Nacional de Ciberseguridad** (INCIBE), ha publicado en la web de is4k (*Internet segura for kids*) unas **guías de mediación parental** para ayudar a las familias mediante recomendaciones y pautas que pueden servirles de apoyo para que los menores lleven a cabo un uso seguro y responsable de Internet. La primera de ellas, corresponde a la ***Guía de mediación parental*** (enlace a PDF).

Copyright 2026



INCIBE. *Guía de mediación parental* (CC BY-NC-SA 4.0)

Por otro lado, también puedes encontrar la ***Guía para uso seguro y responsable de Internet por los menores*** elaborada por INCIBE (pincha aquí para acceder a su página web) y OSI Menores (pincha aquí para acceder a su página web). Puedes descargarte la guía en el siguiente enlace a PDF.

Portada guía mediación parentalIs4k/INCIBE. *Guía uso seguro de Internet por los menores* (CC BY-NC-SA)

Para saber más (Enero 2024)

Menores, salud digital y privacidad. Estrategia y líneas de acción (Agencia Española de Protección de Datos)

¿Qué es el control parental?

Son aplicaciones mediante las cuales los padres o tutores pueden configurar los dispositivos electrónicos con conexión a Internet de modo que los buscadores y plataformas solo ofrezcan a los menores contenidos adecuados a su edad.

- **Este sistema permite:**
  - Establecer horarios de uso y limitar el tiempo de conexión.
  - Monitorizar y obtener información sobre la navegación que se ha realizado en Internet.
  - Evitar que los menores visiten sitios web inapropiados.
  - Evitar su contacto con desconocidos que puedan dar lugar a acciones peligrosas.

¿Qué herramientas podemos utilizar para evitar que los menores accedan a contenidos no deseables?

- **Opciones de filtrado en navegadores**

Google dispone de la Tecnología ***SafeSearch*** capaz de bloquear resultados explícitos. Puede ayudarte a filtrar contenido explícito de los resultados, incluyendo contenido sexual, pornografía, imágenes sangrientas y violencia que no va dirigida a un público infantil. No es infalible, pero, aproximadamente, se consiguen excluir este tipo de contenidos en 70 de cada 100 búsquedas. Puedes activarlo siguiendo estos pasos:

- Accede a **Configuración** de Google.
- Haz clic en la primera opción **Configuración de búsqueda**.
- Dentro de **Filtros Búsqueda Segura**, selecciona la opción que creas conveniente:
  - **Mostrar resultados explícitos** para desactivar SafeSearch.
  - **Ocultar resultados explícitos** para activar SafeSearch.

- **Programas que filtran o bloquean el acceso a contenidos no deseados**
  - Naomi Family Safe Internet.
  - K9 Web Protection.
- **Programas de monitorización y registro** de uso del ordenador:
  - PC TimeWatch.
- **Sistemas operativos** que que permiten que el ordenador solo pueda usarse en una determinada **franja horaria**.

Windows o Android, pueden configurarse y establecer las restricciones al uso del dispositivo mediante la opción **Control parental**.

- Programas de **filtrado de salida** ayudan a proteger los datos que el usuario de un ordenador sube a Internet, como los datos personales, y monitorean y restringen el flujo de información saliente. Los paquetes que están siendo enviados fuera de la red interna son inspeccionados por medio de un *router*, *firewall*, etc. A los paquetes de información que no cumplen los protocolos de seguridad se les impide la salida.

Es conveniente que los adultos revisen el historial de navegación del menor con cierta frecuencia, comprobando qué páginas ha visitado y para qué, siempre **salvaguardando la intimidad del menor** y la **confidencialidad de sus datos**.

A continuación, el **vídeo *Controles parentales en el hogar*,** publicado por is4k, ofrece algunas referencias para llevar a cabo un buen control parental:

Copyright 2026

https://www.youtube.com/embed/aV2rvAGTQSE

YouTube / is4k. *Controles parentales en el hogar* (Licencia de YouTube estándar)

Puedes obtener más información específica acerca de este tema en la guía creada por INCIBE y publicada en la web de is4K ***Guía de herramientas de control parental*** (enlace).

¿Qué cuidados básicos requieren los equipos digitales para su correcto funcionamiento?

Es importante conocer cómo llevar a cabo el mantenimiento de las herramientas y dispositivos de ocio o trabajo digital, evitando riesgos físicos, con el objetivo de asegurar su buen funcionamiento y prolongar su vida útil, lo cual contribuirá colateralmente a la defensa del medio ambiente.

A continuación, podrás ver **algunas de las medidas** que debes tener en cuenta:

- La **limpieza** debe realizarse cuidadosamente utilizando productos de limpieza neutros indicados para tal fin o un paño ligeramente humedecido.
- Cuando termines de utilizarlo, debes **esperar el tiempo necesario** antes de retirar el cargador de modo que el apagado se realice correctamente evitando que se produzcan daños internos.
- Si observas un **funcionamiento anómalo** de tu dispositivo, consulta a un informático o especialista antes de que se produzcan daños irreversibles.
- Es importante **no golpear el ordenador** bruscamente y protegerlo ante caídas. Si es portátil, abatir la pantalla con cuidado y no colocar peso sobre el mismo.
- **Evitar derramar comida o bebida** sobre el teclado, alejarlo de focos de calor, no exponerlo largo tiempo al sol u otros tipos de radiaciones, así como protegerlo de material imantado.
- **No instalar *software*** que incumpla las medidas de seguridad y pueda poner en peligro su correcta utilización.
- Situarlo en una **superficie plana** y estable, sin vibraciones, limpia de productos químicos y de polvo que puedan filtrarse a su interior y, a ser posible, no brillante (evitando las de cristal) y de color claro.

¿Es importante prestar atención a la ergonomía informática?

Cuando se habla de **ergonomía informática**, se hace referencia a la búsqueda de la comodidad postural saludable que debe adoptarse cuando usamos dispositivos digitales. Las siguientes recomendaciones contribuirán a tu bienestar digital.

- **Posición del cuerpo**

Copyright 2026

- Es conveniente **sentarse correctamente** sobre una silla regulable en altura y con respaldo en el que pueda apoyarse toda la espalda, evitando tensiones.
- **Relajar los hombros** realizando movimientos circulares cada cierto tiempo, echándolos hacia atrás y hacia abajo.
- Tener **conocimientos sobre mecanografía** y escribir sin mirar al teclado puede ayudarnos a no sobrecargar las cervicales.
- Al menos cada 2 horas, se debe **tomar una pausa**, levantarse, y estirarse al mismo tiempo que se realiza una respiración profunda. Todo esto nos permitirá liberar tensiones. En el caso de tratarse de un menor, este periodo de tiempo debería reducirse a 1 hora.

- **Posición de las manos**
  - Los teclados inclinables independientes son **más ergonómicos** que los integrados de los portátiles.
  - Para **evitar daños o lesiones** en las muñecas y en las manos, debemos seguir las indicaciones relativas a la forma de coger y mover el ratón.
  - El estado de ánimo también influye en la tensión muscular pudiendo causar lesiones en forma de tendinitis, capsulitis o contracturas que no se producirían si la persona estuviera trabajando contenta y relajada.
- **Posición de los ojos**
  - La parte central de la **pantalla** debe permanecer formando un ángulo de 20º por debajo de la línea horizontal que une los ojos con la parte superior del monitor y manteniendo una distancia de 50-60 cm al plano de ésta.
  - Es recomendable **enfocar la vista** en un punto lejano cada 30 minutos.
  - Si se tratara de un menor, debe acostumbrarse a **levantar la vista** de la pantalla cada periodo de 15 o 20 minutos.
  - **Cerrar los ojos y cubrirlos con las palmas** de las manos sin presionarlos, te permitirá sentirlos relajados.
  - La **resolución de pantalla y tamaño** de letra han de ser lo suficientemente grandes para que nos permita trabajar de forma cómoda y manteniendo la distancia adecuada.
  - Buscar posiciones y ubicaciones en las que la **luz** sea **adecuada**, evitando reflejos, alto contraste entre la pantalla y la oscuridad del ambiente, etc.

En la siguiente infografía se resumen todos estos aspectos que acabamos de citar:

Chico sentado al ordenador

Mª Elena Sanz Velázquez. *Ergonomía informática* (CC BY-SA)

6.4.2. Reciclaje de dispostivos

En este punto nos centramos en la segunda parte del indicador B2 basado en cuidar los equipos de forma adecuada para aumentar su vida útil y definir un método de reutilización o reciclaje para reducir el impacto medioambiental que producen.

¿Es conveniente reflexionar sobre este aspecto?

Es importante como adultos ser conscientes de los efectos que el uso de las nuevas tecnologías conlleva sobre el planeta. Conocer cómo afectan los materiales que las componen al medio ambiente, también es muy recomendable, tanto en lo que se refiere a su **extracción** como en cuanto a las posibilidades de **reciclaje** una vez que haya finalizado la vida útil del producto tecnológico. Muchos de los componentes con los que se fabrican los dispositivos electrónicos están siendo sobreexplotados y constituyen materiales finitos que no se deben malgastar. Algunos, incluso, se agotarán en unas décadas. Por ello es crucial impulsar una **cultura del reciclaje y la reutilización** que aproveche al máximo la vida útil de los equipos.

Es crucial que tanto las familias como los educadores reflexionen conjuntamente acerca del impacto que esto provoca sobre el planeta; los menores podrán asumir su parte de **responsabilidad**, valorarlo y ser conscientes respecto al buen uso, correcto mantenimiento y cuidado de dicho material. Desde los centros educativos, se incluye esta temática aprovechando la transversalidad dentro de la educación en valores, pero deben ser las familias las encargadas de **tomar decisiones** en cuanto a la adquisición de material tecnológico digital para el consumo del estudiante.

Ante la vertiginosa evolución de las tecnologías de la información y la comunicación, siempre conviene racionalizar y analizar si la elección de un producto está fundamentada en las necesidades reales del menor o, por el contrario, en un engañoso *marketing* o en la posible búsqueda de un ilusorio **prestigio social** dentro de su grupo de iguales. Un objetivo capital de la sociedad debe consistir en proteger a los menores de verse envueltos en una espiral de consumo y de desear poseer las **últimas novedades** en cuanto a herramientas digitales, dispositivos y sus complementos.

Se debe conocer que existen multitud de servicios y programas gratuitos que pueden sustituir exitosamente a los de pago, con funcionalidades más que suficientes para las necesidades del

Copyright 2026

alumnado. Algunos sociólogos ya han dado un nombre a esta tendencia sobre el consumo indiscriminado de material digital, denominándolo con el término ***tecnonarcisismo***.

¿Qué entendemos por dispositivo electrónico?

Podemos definir el término, **dispositivo electrónico** como aquel aparato formado por una combinación de componentes electrónicos, organizados en circuitos, con capacidad de utilizar las señales eléctricas para realizar procesos **informáticos**. A continuación, se recogen algunos **ejemplos:**

- Teléfonos inteligentes o *smartphones*
- Tabletas
- Ordenadores portátiles personales, o de sobremesa
- Relojes inteligentes
- Reproductores digitales
- Cámaras
- Dispositivos GPS
- Videoconsolas.

¿En qué consiste el reciclaje de un dispositivo electrónico?

Cuando un dispositivo electrónico se queda obsoleto, deja de funcionar o es descartado por su usuario, pasa a convertirse en un deshecho y, como tal, debe **integrarse en un proceso de reciclaje** consistente en desmontaje y separación de sus diferentes componentes con la finalidad de recuperar las materias primas que lo componen, incluso reutilizarlas en caso de ser posible.

¿Por qué debemos reciclar los dispositivos electrónicos?

Reciclar dispositivos electrónicos tiene muchos **beneficios, tanto a nivel económico, como social y medioambiental**. Este tipo de aparatos, contienen metales pesados muy contaminantes en diferentes proporciones tales como el plomo, mercurio y cromo por lo que deben tratarse correctamente para evitar que lleguen a ser peligrosos para la salud y que materiales tóxicos vayan a parar a la atmósfera o a las vías fluviales. Cada día se generan gran cantidad de deshechos electrónicos, llegando a acumular anualmente unos 50 millones de toneladas de basura electrónica de la que tan sólo se consigue reciclar un 20%, aproximadamente.

El reciclaje permite **recuperar elementos** como vidrio, plástico y metales que pueden volver al ciclo productivo, disminuyendo la cantidad de extracción y contribuyendo al equilibrio medioambiental, pues se reduce la contaminación del aire, suelo y agua.

En cuanto a las **ventajas económicas**, se puede contemplar la reducción de costes gracias a la recuperación de algunos materiales y reincorporación al proceso productivo, llevando consigo

Copyright 2026

además generación de empleo debido a la creación de nuevos puestos de trabajo.

¿Cómo podemos realizar tareas de reciclaje de dispositivos en un centro escolar?

Cuando un dispositivo queda obsoleto para utilizarlo con determinadas herramientas que requieren de más capacidad o potencia, se puede destinar a la realización de búsquedas en Internet. Una opción es crear un **rincón digital** en el aula, de manera que el alumnado pueda buscar información a través de la red para las tareas diarias.

Otros dispositivos digitales que ya no funcionan, pueden ser utilizados en áreas relacionadas con la digitalización para proceder al desmontaje como parte de una tarea colaborativa llevada a cabo por grupos de estudiantes de modo que les permita **comprender el funcionamiento de los diferentes componentes**, su composición, así como el **impacto que estos producen sobre el medio ambiente**.

Por último, se debe solicitar, a través del organismo correspondiente, la recogida de los deshechos digitales generados en el centro para que sean gestionados en una **planta de reciclaje**.

Copyright 2026

6.4.3. Ejemplos de aplicación

La metodología de aprendizaje dentro de una educación digitalizada se basa en que el alumnado pueda **aprender de forma más autónoma**, aunque siempre guiado por el docente. El profesorado debe colaborar en el desarrollo de la capacidad de los estudiantes para **buscar, filtrar, interpretar y comunicar la información**, tanto de forma individual, como en entornos de cooperación entre iguales, valiéndose de las oportunidades que proporcionan las nuevas tecnologías y aprovechando las posibilidades de aprendizaje y de comunicación que nos ofrece **Internet** .

Las **herramientas y recursos didácticos digitales** educativos constituyen una oportunidad para desarrollar un aprendizaje más motivador y eficaz, permitiendo el acceso a múltiples y variadas fuentes de información mediante el empleo de herramientas multimedia e interactivas. La finalidad consiste en lograr una **educación de calidad**, comprometida con las necesidades de la sociedad del conocimiento, más actualizada y, sobre todo, más **cercana al entorno del alumnado**.

Uno de los objetivos del sistema educativo actual es la adquisición de la **competencia digital**, es decir, la obtención de conocimientos, habilidades y capacidades, en armonía con **valores y actitudes**, utilizando de manera óptima y eficaz, en todas las áreas de conocimiento, las herramientas y recursos tecnológicos digitales.

La **dinamización del aprendizaje motivacional** puede conseguirse gracias a la coexistencia de gran variedad de herramientas, muchas de ellas *online,* pues permiten al alumnado realizar el aprendizaje a través de otras actividades educativas como, por ejemplo, diseñar infografías, montar vídeos y alojarlos en una red educativa, crear radios escolares, mapas de conceptos, libros electrónicos en la red, ejes cronológicos, mapas de etiquetas describiendo los lugares señalados, posters multimedia o revistas digitales, entre otras. Todos estos recursos digitales deben estar integrados en el marco de una enseñanza global, activa y participativa.

Actividades de privacidad y seguridad

Vídeos
El mago de las redes sociales: En ocasiones, los poderes adivinatorios tienen menos misterio del que puede parecer, basta con no configurar nuestra privacidad en RRSS.

Copyright 2026

https://www.youtube.com/embed/lVvfx0GT5sk

Videos de la Agencia Española de Protección de Datos: Tú controlas en internet.

Privacidad en RRSS:

https://www.youtube.com/embed/D57vDI7w_mA

Privacidad:

https://www.youtube.com/embed/-x1-hdcF2TU

Videos para trabajar la privacidad en RRSS en secundaria:

https://www.youtube.com/embed/Ak3qp4qRAiY

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

https://www.youtube.com/embed/we7wO2PJJfQ

Secuencia didáctica 1: "A la caza del tesoro en Instagram"

A continuación os vamos a compartir un **perfil de Instagram de una adolescente** (por supuesto ficticio), donde veremos la cantidad de datos que se pueden encontrar. Se trata de una actividad bastante ilustrativa para realizar con alumnado de secundaria. Observando un perfil que podría ser el de cualquier alumno nuestro, podremos encontrar datos como:

- Instituto donde estudia
- Nombre de una de sus mejores amigas.
- Calle y portal donde vive.
- Nombre de su perro y lugares por donde lo pasea.
- Biblioteca donde estudia y donde estará cada tarde durante unos cuantos días.
- Actividad extraescolar que realiza, donde la realiza y en qué horario.
- Punto de encuentro los fines de semana por la noche con sus amigos.

Actividad extraída de www.internetsegura.cat

Secuencia didáctica 2: Creamos una contraseña segura que sea fácil de recordar

Es importante que el alumnado aprenda a crear contraseñas robustas y fáciles de recordar, de modo que no queden expuestas o vulnerables frente a terceras personas.

Durante una sesión de tutoría, se ayuda a los alumnos a crear una contraseña segura intentando aportar trucos o ideas que puedan servirles de ayuda. El objetivo es crear una **contraseña** para entrar nuestro EVA En dicha sesión, se puede establecer la siguiente secuencia:

1. Plantea un **juego de contraseñas en el aula**: con dos mesas ligeramente separadas crea una especie de barrera. A modo de guardas de seguridad, un alumno y una alumna se sentarán a ambos lados, sobre las sillas correspondientes a cada uno de los pupitres. Todos los demás estudiantes se colocarán a un lado de la barrera y solo podrá pasar al otro lado de las mesas aquel alumnado que sea capaz de repetir la contraseña previamente indicada por cada uno de los guardianes. Esta operación la realizarán de forma alterna. Los caracteres serán sustituidos por palmadas, pequeños golpes o gestos y se irán realizando en diferentes rondas con los ganadores. Al principio, constarán de tres señales, después de cinco e iremos aumentando progresivamente. Cada vez fallarán más alumnos que no podrán pasar debido al aumento de dificultad. Con ello, se pretende demostrar a los alumnos que una contraseña larga será más difícil de adivinar por un ciberdelincuente.

2. Realiza una **búsqueda en Internet de contraseñas no seguras** para que nunca las elijan como propias. A modo de ejemplo, a continuación encontrarás el ranking de contraseñas más vulnerables:
   - 12333456
   - password

- ABC123

3. Ofrece algunas de las pautas adaptándolas a su edad para que puedan **crear su propia contraseña**. A continuación, se repiten las claves para crear contraseñas más seguras a partir de la **utilización de caracteres** que se explicaron en el punto 1.1. de este módulo:
   - Incluir letras, números y símbolos.
   - Alternar mayúsculas y minúsculas.
   - Incluir caracteres especiales (~! @ # $% ^& * -+ = ‘ | \ \( ) { }\ [ ]:; “’ < >,.? /).:
   - Tener una longitud igual o mayor a 10 caracteres (aconsejable 12).
   - No tener números ni letras consecutivas.
   - Sustituir algunas letras por cifras, i por 1, e por 3, o por 0, etc.
   - Que no sea similar a contraseñas anteriores.
   - Que utilice frases complejas en estructura, pero fáciles de recordar.
   - Debes cambiarlas con cierta frecuencia, recomendable cada 3 meses.
   - Utilizar una para cada servicio de Internet.
   - Usar palabras poco comunes o inusuales.
   - Deben tener poca o ninguna relación con los datos de la persona a quien protegen.
   - No compartirlas con nadie, ni amigos ni familiares.

Otra posibilidad es recurrir a **canciones o citas populares** para que sea más fácil de recordar como, por ejemplo, recordar las dos primeras letras de cada palabra dentro de una frase. Tienen que hacer diferentes combinaciones usando la imaginación. Siempre se intentará aumentar la complejidad no dando pistas a aquellos que intenten adivinarlas.

Secuencia didáctica 3: Revisamos los permisos solicitados por las aplicaciones

Tanto nosotros como el alumnado, a menudo realizamos la **instalación de aplicaciones en los dispositivos móviles** y, en ocasiones, por desconocimiento se otorgan permisos que no son necesarios para la funcionalidad de estas aplicaciones. También existen **aplicaciones no fiables** y, si se llegas a instalar, debemos saber cómo actuar. Se debe concienciar al alumnado de que **los usuarios** son la **primera línea de defensa** frente a las amenazas, por lo que hay que usar siempre el sentido común y estar atentos para no conceder más permisos de los necesarios, evitando los riesgos de acceso a la privacidad que conlleva.

Como objetivo de esta actividad, se pretende desarrollar el **espíritu crítico y la autoconfianza** basada en el conocimiento. Para llevarla a cabo, te puedes apoyar en una de

las campañas de concienciación sobre el **uso de seguro de dispositivos móviles,** lanzada por la Oficina de Seguridad del Internauta (OSI), así como en infografías y material relacionado con la privacidad y la seguridad dentro del entorno digital.

1. Apóyate en la web de la OSI, dentro del apartado **¿Por qué piden tantos permisos las apps?** (enlace), y comenta en el aula los tipos de permisos que suelen pedir las aplicaciones y las consecuencias que tiene conceder cada uno de ellos. Algunos de los permisos que suelen pedir las aplicaciones antes de instalarse son el acceso al teléfono, al almacenamiento, a la memoria, a los mensajes de texto, al calendario, a la cámara, a tus contactos, a tu ubicación, al micrófono y a los sensores corporales. A veces, estos permisos no son obligatorios y los desarrolladores buscan extraer información sobre el usuario para poder enviar publicidad personalizada. Si se trata de de una aplicación con fines ilícitos, aprovecharían para acceder y robar tu información privada y confidencial almacenada en el dispositivo, así como los datos de acceso a tus contactos, etc. Los estudiantes deben conocer que, por ejemplo, al dar permisos de acceso al almacenamiento o memoria del dispositivo, podrían proceder al cifrado de los archivos que contienen, pidiendo un rescate o extorsión para permitir recuperarlos.

2. Emplea la **infografía descargable** (enlace) que ofrece la Oficina de seguridad del internauta (OSI), que incluye una tabla en la que puedes ver, con cada permiso que autorizas a la aplicación, los datos personales que directa o indirectamente estas proporcionando, así como los posibles riesgos que esto conlleva, debido a que:

    - La aplicación puede tener **malas intenciones**.
    - La aplicación puede sufrir algún **error.**
    - La aplicación puede ser víctima de un **ciberataque**.

Copyright 2026

¿Debo darle acceso a esta app a mis contactos?

¿O a mis SMS? ¿Y al micrófono?

Este interrogante se nos presenta una y otra vez cada vez que instalamos alguna aplicación, pero **¿sabemos realmente las consecuencias que puede tener para nosotros un uso fraudulento de los permisos que concedemos?**

Principales permisos y riesgos para nuestra privacidad y seguridad

Con cada permiso que damos, **proporcionamos información sobre nosotros.** Si la app tiene malas intenciones, sufre algún error, o un ciberataque, puede ponernos en riesgo.

Riesgos	Calendario Conocer y cambiar nuestras citas, fechas, reuniones y rutinas.	Contactos Acceder a nuestra lista de contactos y ver la lista de cuentas de servicios.	Cámara Micrófono Realizar grabaciones de vídeo, audio o tomar fotografías.	Memoria Acceder o modificar cualquier archivo o dato almacenado.	Mensajes De texto Acceder, modificar, o enviar mensajes SMS.	Sensores Del cuerpo Conocer datos sensibles sobre nuestra salud y actividad física.	Teléfono Acceder al histórico de llamadas y funcionalidades del teléfono.	Ubicación Conocer nuestra ubicación en tiempo real.	Otros permisos Que debemos revisar por no estar excentos de riesgos.
Suplantación de identidad	✓	✓	✓	✓	✓				
Robo de datos personales y confidenciales	✓			✓	✓		✓		
Publicidad dirigida	✓		✓			✓		✓	
Ataques de ingeniería social y phishing	✓	✓		✓	✓	✓	✓	✓	
Riesgo para la seguridad física	✓							✓	
Envío de spam, fraudes y malware		✓			✓		✓		
Pérdida de privacidad			✓					✓	
Extorsión/sextorsión			✓	✓					
Suscripción a servicios premium					✓		✓		
Difusión de datos sobre el estado de salud						✓			
Administradores del dispositivo: control total del dispositivo									✓
Instalar aplicaciones									✓

OSI / INCIBE. *Principales permisos y riesgos para nuestra privacidad y seguridad* (CC BY-NC-SA)

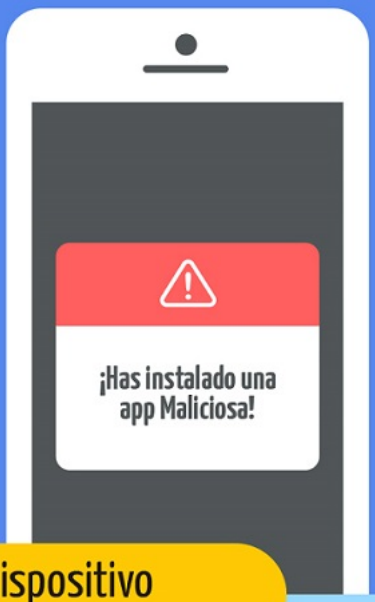
3. Usa otro **recurso de INCIBE descargable desde la web de la OSI** (enlace) que explica el protocolo de actuación en el **caso de haber instalado una aplicación no fiable**.

¡AYUDA!

Instalé una app no fiable

¿Alguna vez te has descargado una aplicación móvil maliciosa o no fiable?

Estás buscando una aplicación de la que has oído hablar por Internet.
De pronto, la encuentras a través de un enlace de descarga de una web, la instalas y la inicias. Sin embargo, no ocurre lo que esperabas y tu dispositivo empieza a actuar de forma extraña.



¿Qué puedes hacer?

El primer paso es desinstalarla del dispositivo. Tener en cuenta las siguientes recomendaciones para que esto no te vuelva a suceder.

Prevención y protección de tu dispositivo

Ten un **antivirus** instalado

Protege tu dispositivo de diversas amenazas y aplicaciones maliciosas.
En la sección de herramientas gratuitas de OSI encontrarás algunas para Android e iOS.

www.osi.es



Haz copias de seguridad

Pueden estar en la nube con Google Drive (Android) o iCloud (iOS), o en nuestro ordenador sincronizadas con el dispositivo móvil.

Cifra tu dispositivo

****

Protege la información del dispositivo haciéndola menos accesible desde las opciones de seguridad que ofrecen Android e iOS.

DESCARGA

En tiendas oficiales

Las plataformas Google Play o AppStore cuentan con medidas de seguridad para evitar aplicaciones fraudulentas.

Descarga Disponible Google play

Descarga Disponible App Store



OSI / INCIBE. *Instalé una app no fiable* (CC BY-NC-SA)

4. Para terminar, utiliza un recurso pedagógico, enmarcado dentro de la campaña sobre la correcta utilización de los dispositivos móviles, en la que de un modo práctico los alumnos deben elegir "**Acepto o no acepto**" (enlace) a las peticiones que solicitan las aplicaciones durante la instalación.

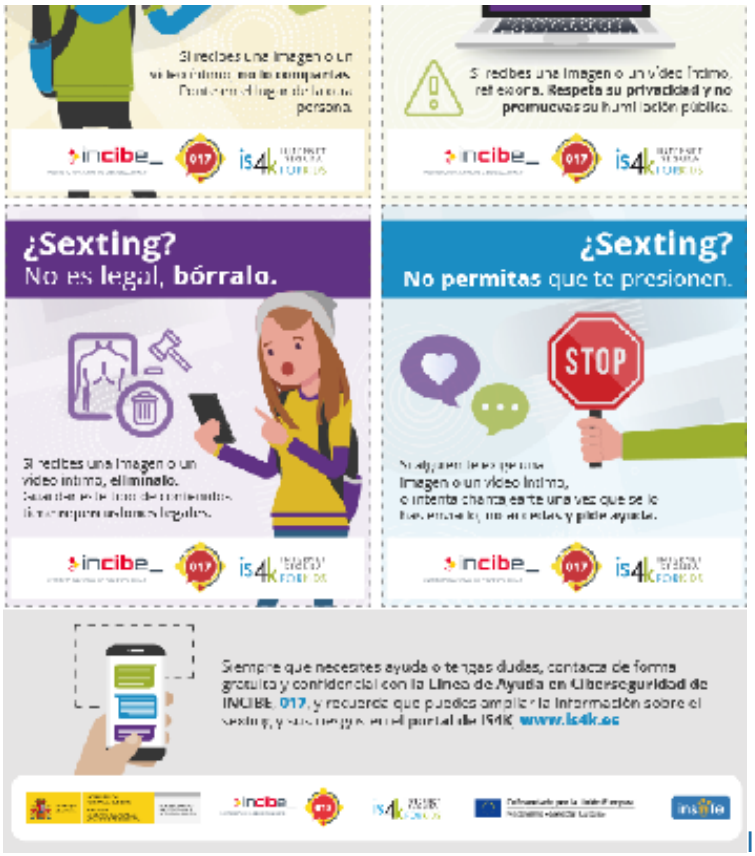
En dicha actividad, se muestra una **simulación** de petición de permisos que solicitan cinco aplicaciones muy diferentes entre sí. Los alumnos, deberán elegir cuáles deben aceptar y cuáles denegar sin interferir en el correcto funcionamiento de la misma. Después de contestar, se les mostrará **qué respuesta era la acertada** y las razones que lo justifican.

Ciberacoso

Se puede tratar como **tema transversal** en la mayor parte de las áreas, pero más específicamente en Tutorías o dentro de las más relacionadas con temas de digitalización. Las actividades deberían estar coordinadas desde el Departamento de Orientación.

Prevención frente al sexting

- : una parte de los integrantes del equipo de "**alumnos-ayuda**" coloca, en lugares que ellos consideren estratégicos dentro del centro, carteles que contengan indicaciones para protegerse frente al *sexting.* Pueden diseñarlos ellos mismos tomando como modelo el que encontramos en la web específica sobre seguridad digital is4k (enlace).



Is4k / INCIBE. *No difundas* (CC BY-NC-SA)

Todos los miembros del equipo de "**alumnos-ayuda**" elabora una **infografía** de forma colaborativa, integrando elementos que capten la atención de sus compañeros mediante la utilización de aplicaciones que les resulten atractivas, como Genially, Canva o similares. En dicha presentación pueden embeber el vídeo que se muestra a continuación:

https://www.youtube.com/embed/8aYMvBzHLso

YouTube / Internet Segura for Kids. *¿Por qué los adolescentes comparten fotos íntimas?* (Licencia de YouTube estándar)

Para ayudarlos a comprender qué razones pueden tener a **nivel biológico o psicológico** para llevar a cabo este tipo de acciones durante la adolescencia, podría ser interesante el visionado del vídeo mostrado a continuación. Esto facilitará la labor de prevención frente al rechazo a su propio cuerpo derivada de la implicación en una situación de este tipo.

En ella, aprovechando el aprendizaje entre iguales ***pair to pair***, se explicaría brevemente en qué consiste el *sexting*, intentando dar una respuesta a los hechos acontecidos y analizando las razones por las cuales las parejas adolescentes lo hacen con más frecuencia. Se debe reflexionar sobre las consecuencias del uso de esas imágenes cuando una pareja se rompe, fijando los riesgos potenciales, responsabilidades y consecuencias a nivel psicológico, ético y legal de estos actos. Se establecerá un protocolo de actuación y se incidirá en la importancia de ejecutarlo con prontitud.

Para concluir la secuencia de actividades y reforzar la asimilación de contenido, puedes establecer un pequeño debate acerca de un caso real de *sexting* publicado en Internet, **analizando en grupo las consecuencias** tanto para el agresor como para la víctima. ¿Cómo puede afectar la falta de control que tiene la víctima sobre de esas imágenes de su cuerpo circulando por las redes a lo largo de su vida?

Se deben explicar las **potenciales acciones legales** que se puedan tomar y, a la vez, entender el sentimiento de culpa e irresponsabilidad que también podría dejar marcado al agresor al interferir en la vida de otra persona, ya que puede no haber sido consciente de las consecuencias de sus actos.

Actividades acerca del uso digital responsable

Trabajamos la ergonomía informática en el aula

1. Se proyecta una **imagen** en el aula en la que se muestrala **postura correcta** de un individuo cuando esté trabajando delante de un ordenador, teniendo también en cuenta la posición de las manos, así como la forma de coger el ratón. Se explica brevemente.

2. Uno de los estudiantes se sienta **imitando la figura de la pantalla** mientras que otro compañero se asegura, utilizando un metro o elemento de medida de ángulos, si realmente está dentro de los márgenes marcados para conseguir una situación de bienestar digital a lo largo del tiempo. Mantener una higiene postural adecuada asegura que no tengas problemas de salud con el tiempo, como problemas de espalda o tendinitis en las manos. En esta actividad, un tercer alumno será el que recuerde los datos que se han de medir, mientras que el resto de la clase observa cómo ha de sentarse.

3. Acto seguido, **agrupados por parejas**, intentarán **conseguir la postura adecuada**, de modo que puedan memorizar la posición cada vez que tengan que utilizar el ordenador, manteniendo la distancia adecuada la pantalla y recordando cómo deben apoyarse en el respaldo de la silla, la altura correcta de su asiento, la posición de los pies, etc. Primero, lo realizará uno de los miembros de la pareja, el otro comprobará la posición y viceversa.

4. Al día siguiente, con todos en el aula de informática, **intentarán recordar** la posición con los datos aprendidos el día anterior y ya **sin la imagen** de la pantalla, deberán saber colocarse adecuadamente en los ordenadores antes de comenzar con la tarea encomendada para ese día.

5. El profesor **valorará el grado de consecución del objetivo** que ha logrado cada alumno, **indicando las correcciones** a realizar en los casos en lo que corresponda.

https://www.educa.jcyl.es/educacyl/cm/gallery/CCD/Area_6/A2.6_Uso_responsable_bienestar_digital/4_aplicacin_en_el_aula.html

Copyright 2026