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.

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**.

¿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 desconocidas: instalación de cualquier app									✓
Acceso a las notificaciones:									

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

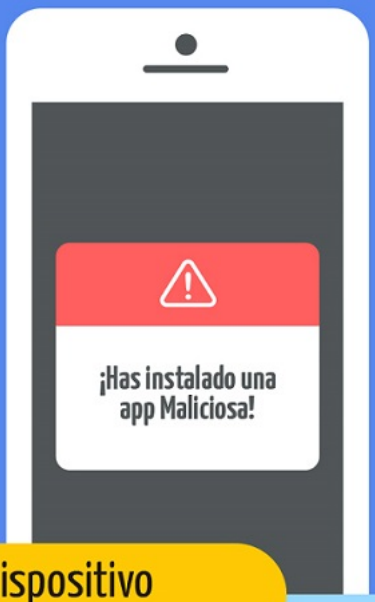
3. Usa otro **recurso de INCIBE descargable desde la web de la OSI** (enlace) que explica el protocolo de actuación en el **caso de haber instalado una aplicación no fiable**.

¡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

1. **Revisa quién es el desarrollador de la app.**

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.

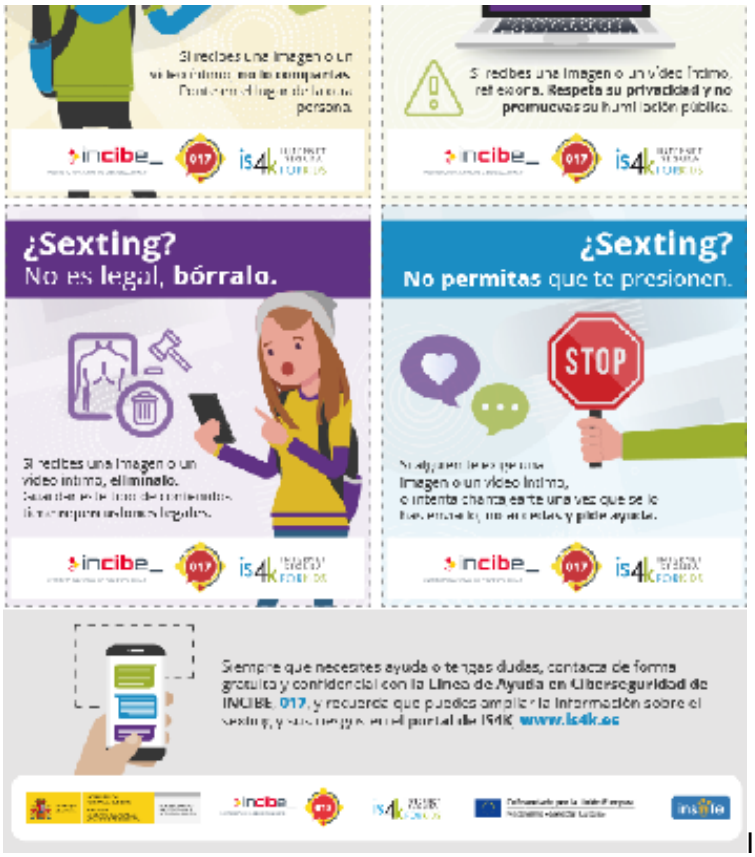
En dicha actividad, se muestra una **simulación** de petición de permisos que solicitan cinco aplicaciones muy diferentes entre sí. Los alumnos, deberán elegir cuáles deben aceptar y cuáles denegar sin interferir en el correcto funcionamiento de la misma. Después de contestar, se les mostrará **qué respuesta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

Revision #2
Created 12 June 2023 09:47:17 by Chefo Cariñena
Updated 19 June 2023 11:26:40 by Chefo Cariñena