CIBERSEGURIDAD Y ADOLESCENTES:
Guía práctica para profesores y padres

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

CONTENIDOS

INTRODUCCIÓN 3

LA PLATAFORMA DIGITAL MOODLE 6

PROGRAMACIÓN DIDÁCTICA: Ciberseguridad para profesores 8

Presentación 9

Modulo 1. Protección de dispositivos y contenidos digitales 10

Modulo 2. Proteger los datos personales y la privacidad 12

Modulo 3. Proteger la salud, el bienestar y el medio ambiente 15

Modulo 4. Perfiles profesionales 17

CIBERSEGURIDAD PARA PADRES: Guía de buenas prácticas 18

Presentación 19

1. Protección de dispositivos y contenidos digitales 20

2. Proteger los datos personales y la privacidad 21

3. Proteger la salud, el bienestar y el medio ambiente 22

Glosario 22

PROGRAMACIÓN DIDÁCTICA SOBRE: Videojuego Be@cyberpro 23

ENLACE ONLINE AL JUEGO 36

PÁGINA DEL PROYECTO 36

REFERENCIAS 37

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

INTRODUCCIÓN

Para una cantidad considerable de ciudadanos europeos, la ciberseguridad sigue siendo un término desconocido. Según datos recientes, muchos europeos aún no han reconocido la importancia de seguir las medidas de ciberseguridad más básicas (Erixon y Lamprecht, 2018; Pupillo, 2018). Por ejemplo, se estima que un 50 % de los profesionales no tiene contraseñas, PIN o seguridad biométrica que proteja sus dispositivos, y el 66,6 % informó de que no contaba con cifrado de datos (Reischuk, 2019). En este contexto, es comprensible que en la última década la Unión Europea (UE) haya decidido desarrollar un fuerte enfoque para mejorar la ciberseguridad en múltiples niveles.

La ciberseguridad podría definirse como "la organización y el conjunto de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados para él de los sucesos que desajustan los derechos de propiedad de jure y de facto" (Craigen, Diakun-Thibault, y Purse, 2014).

Más en concreto, según la Unión Internacional de Telecomunicaciones (UIT), la ciberseguridad abarca el conjunto de herramientas, políticas, conceptos de seguridad, protecciones de seguridad, directrices, enfoques de gestión de riesgos, acciones, formación, buenas prácticas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético y los activos de las organizaciones y los usuarios (Von Solms & Van Niekerk, 2013).

Según la Agencia Europea de Ciberseguridad (ENISA, 2020), los ciberataques son cada vez más sofisticados, selectivos, generalizados y difíciles de detectar. Según esta agencia, el phishing, el robo de identidad y el ransomware han aumentado, sobre todo en el contexto del COVID-19, que ha servido de caldo de cultivo para promover ataques a hogares, empresas, gobiernos e infraestructuras críticas (Kohler, 2020; Sterlini, Massacci, Kadenko, Fiebig, & van Eeten, 2019; Štitilis, Rotomskis, Laurinaitis, Nadvynychnyy, & Khorunzhak, 2020).

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Como resultado, las pérdidas económicas relacionadas con los ciberataques son abrumadoras para los gobiernos, los organismos e instituciones, las empresas y los individuos, que son vulnerables a las crecientes amenazas cibernéticas (Carrapico y Barrinha, 2018; Lis y Mendel, 2019). Se calcula que la ciberdelincuencia cuesta a la economía mundial hasta 575 000 millones de dólares anuales (Sobers, 2019). El aumento de tecnologías disruptivas como el Internet de las cosas, que conecta más de 50 000 millones de dispositivos en la actualidad, ha aumentado enormemente el riesgo potencial de ciberataques (Lis y Mendel, 2019).

En este contexto, parece razonable plantearse una importante inversión de recursos económicos y humanos que sean capaces de hacer frente a esta amenaza. Sin embargo, poco se hace ante la falta de recursos disponibles y de capital humano que pueda hacer frente a dicha amenaza. Se prevé que, para 2021, habrá 3,5 millones de puestos de ciberseguridad sin cubrir (Ventures, 2017). Por lo tanto, las organizaciones tendrán que enfrentarse al reto de contratar a profesionales y expertos en ciberseguridad en un mercado laboral en el que escasean los profesionales con las habilidades y la formación adecuadas para satisfacer las demandas del mercado (Crumpler y Lewis, 2019).

Además, la baja proporción de mujeres cualificadas que trabajan en el sector de la ciberseguridad podría agravar el problema. Según datos recientes, la proporción de mujeres empleadas en este sector en Europa es del 7 %, lo que está lejos de la igualdad de género que exigen las necesidades actuales del mercado (Poster, 2018). Los estereotipos de género, la discriminación y un entorno de trabajo muy masculinizado podrían estar detrás de la brecha de género en ciberseguridad (Bagchi-Sen, Rao, Upadhyaya y Chai, 2010; Poster, 2018). La literatura existente indica que las mujeres se enfrentan a muchas barreras para entrar y progresar en el sector; desafíos sociales, institucionales y personales (Bagchi-Sen, et al., 2010). La cultura androcéntrica desempeña un papel importante en las decisiones de las mujeres de cursar estudios superiores de informática (Heaton y McWhinney, 1999). En este contexto, las estudiantes tienen escasas opciones de orientación y tutoría, a pesar de que esas oportunidades desempeñan un papel crucial a la hora de fomentar su entrada en el mercado laboral de la informática (Ahuja, 2002; Parasuraman, Purohit, Godshalk y Beutell, 1996).

La formación, el interés y las habilidades, y la identificación con las TI pueden chocar con diferentes aspectos de la identidad del rol femenino, lo que influiría negativamente en la creencia de la mujer en su capacidad para tener éxito en el sector (Trauth, Quesenberry y Morgan, 2004).

Project number: 2018-1-ES01-KA201-05046

Co-funded by the Erasmus+ Programme of the European Union

Además, se ha comprobado que la dificultad para conciliar las responsabilidades profesionales y familiares es una barrera considerable en su avance profesional (Armstrong, Riemenschneider, Allen y Reid, 2007). Teniendo en cuenta que el futuro de la ciberseguridad depende de su capacidad para atraer y retener a las mujeres, la promoción de su participación en la ciberseguridad debe entenderse como una prioridad en la actualidad (Poster, 2018). Se podría potenciar su presencia en el sector de las TI minimizando las barreras en las primeras etapas de la carrera de las mujeres, asegurando la igualdad de oportunidades en el acceso a los títulos de TI y promoviendo su avance profesional en TI, así como sus habilidades técnicas y analíticas.

Estos aspectos podrían, a su vez, contribuir a una mayor presencia de modelos femeninos que guíen e inspiren a las jóvenes a involucrarse en este campo (Bagchi-Sen, et al., 2010).

Por todas estas razones, Be@CyberPro es un proyecto de la UE dedicado a eliminar las carencias de competencias y de género en el sector de la ciberseguridad mediante la formación, la inspiración de las alumnos (especial, pero no exclusivamente), la capacitación de los profesores y la participación de los padres. El objetivo de Be@CyberPro es abordar la brecha de género colaborando con empresas del sector privado e instituciones académicas y trabajando con centros de secundaria, bachillerato y formación profesional para promover las carreras de ciberseguridad. El principal grupo objetivo del proyecto es el alumnado de secundaria y de formación profesional reglada en general, y las chicas en particular. En segundo lugar, los profesores y las familias se verán afectados. Hacer que la información sobre las carreras de ciberseguridad esté más disponible para los estudiantes, los profesores y los padres podría afectar positivamente a más jóvenes a la hora de elegir este camino. Además, tener acceso a información sobre modelos femeninos positivos puede ayudar a motivar a las jóvenes a seguir con su pasión.

Este es precisamente el objetivo de este libro: difundir entre docentes y familias algunos de los resultados más destacados de nuestro proyecto.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

LA PLATAFORMA DIGITAL MOODLE

Se ha desarrollado un curso online en Moodle con los contenidos básicos de seguridad informática para profesores, con el fin de que tengan los conocimientos adecuados para enseñar seguridad informática a sus alumnos y conocimientos de la profesión para poder orientarlos.

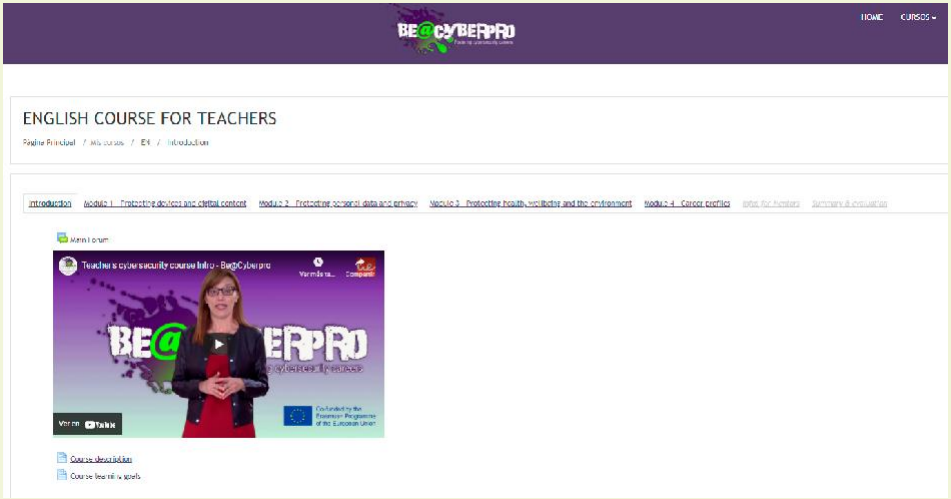


Figura 1. Pantallazo del curso de Ciberseguridad para profesores en la plataforma Moodle.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Moodle es un sistema de gestión de cursos (CMS), también conocido como sistema de gestión del aprendizaje (LMS) o entorno de aprendizaje virtual (VLE). Es una aplicación web gratuita que los docentes pueden utilizar para crear sitios de aprendizaje en línea eficaces. Se ha hecho muy popular entre los educadores de todo el mundo como herramienta para crear sitios web dinámicos en línea para sus alumnos. Para que funcione, es necesario instalarlo en un servidor web en algún lugar, ya sea en un ordenador propio o en uno de una empresa de alojamiento web.

- El objetivo del proyecto Moodle es siempre dar a los educadores las mejores herramientas para gestionar y promover el aprendizaje, pero hay muchas maneras de utilizarlo: tiene características que le permiten escalar a despliegues muy grandes y cientos de miles de estudiantes, pero también puede usarlo un colegio de primaria o un aficionado de la educación. Muchas instituciones lo utilizan como plataforma para impartir cursos totalmente en línea, mientras que otras lo utilizan simplemente para complementar los cursos presenciales (lo que se conoce como aprendizaje mixto).

Muchas instituciones lo utilizan como plataforma para impartir cursos totalmente en línea, mientras que otras lo utilizan simplemente para complementar los cursos presenciales (lo que se conoce como aprendizaje mixto).

- A muchos de nuestros usuarios les encanta utilizar los módulos de actividad (como foros, bases de datos y wikis) para construir comunidades de aprendizaje con una rica colaboración en torno a su materia (en la tradición del construccionismo social), mientras que otros prefieren utilizar Moodle como una forma de entregar contenidos a los estudiantes (como los paquetes SCORM estándar) y evaluar el aprendizaje mediante tareas o cuestionarios.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

PROGRAMACIÓN DIDÁCTICA:
Cibersecuridad para profesores

ÍNDICE

Presentación 9

Modulo 1. Protección de dispositivos y contenidos digitales 10

Modulo 2. Proteger los datos personales y la privacidad 12

Modulo 3. Proteger la salud, el bienestar y el medio ambiente 15

Modulo 4. Perfiles profesionales 17

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

PRESENTACIÓN

Puedes utilizar el material didáctico elaborado por Be@CyberPro en tus clases para trabajar con tus alumnos. El objetivo es mejorar su competencia digital y, sobre todo, generar un comportamiento responsable e informado en consonancia con los principios básicos de la ciberseguridad.

Este programa ofrece una propuesta para trabajar con los alumnos a partir de estos materiales. Se puede trabajar todo el contenido o seleccionar módulos individuales.

El tiempo recomendado en esta programación es de 8 sesiones de una hora. De 1 a 3 sesiones de trabajo para cada uno de los módulos o bloques de contenidos. Para los alumnos de ESO y Bachillerato, las sesiones de tutoría grupal pueden ser un espacio perfecto para poner en práctica estas propuestas didácticas en el caso de que no impartas asignaturas específicamente centradas en las tecnologías digitales. Ahora bien, también puedes utilizar este programa en otras materias.

CONSEJOS PRÁCTICOS ANTES DE EMPEZAR

- Presenta cada tema a tratar mediante un diálogo con los alumnos. Haz preguntas abiertas que les permitan compartir experiencias e inquietudes entre ellos.
- Puedes utilizar otros recursos para introducir un tema, como, por ejemplo:
  - Noticias de actualidad.
  - Extractos de películas.
  - Extractos de una serie dirigida a su grupo de edad
- Speak honestly, without minimising or softening the risks but without exaggerating. Prevention begins with knowing the truth
- Trabajos de casos reales que se acerquen a las necesidades e intereses de los alumnos. No lo hagas todo tú. Invita a expertos en ciberseguridad para que los alumnos conozcan otras realidades.
- Habla con sinceridad, sin minimizar ni suavizar los riesgos, pero sin exagerar. La prevención empieza por saber la verdad.
- Fomenta su pensamiento crítico contrastando información o realizando actividades en las que puedan compartir sus ideas y opiniones.
- Utiliza material variado. Además de los que hemos sugerido, puedes encontrar más material en espacios educativos online como https://www.betterinternetforkids.eu/. También existe una red de Centros de Internet Segura (SIC) en toda Europa, que suele incluir un centro de sensibilización, una línea de ayuda, una línea telefónica y un panel de jóvenes

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

MODULO 1. PROTECCIÓN DE DISPOSITIVOS Y CONTENIDOS DIGITALES

OBJETIVOS

- Ser capaz de diferenciar una gran variedad de riesgos y amenazas en los entornos digitales: noticias falsas, ransomware, phishing, spam, grooming, sexting, violación de derechos de autor, etc.
- Saber aplicar medidas de seguridad y protección y guiar a otros (compañeros y estudiantes) para que las apliquen.

COMPETENCIES BASED ON DigComp FRAMEWORK

4.1. Competencias basadas en el Marco DigComp

Conocimiento:

- C1. Riesgos y amenazas avanzadas en entornos digitales.
- C2. Medidas avanzadas de protección de dispositivos digitales: uso de antivirus, antimalware, filtros antispam, contraseñas, actualizaciones de software.
- C3. Información personal. Niveles de protección según la naturaleza de los datos.

Habilidades:

- H13. Puedo aplicar diferentes formas de proteger los dispositivos y los contenidos digitales y guiar a otros para que lo hagan.
- H14. Soy capaz de diferenciar una amplia variedad de riesgos y amenazas en entornos digitales: fake news, ransomware, phishing, spam, grooming, sexting, violación de derechos de autor, espionaje industrial, etc.
- H15. Sé aplicar medidas de seguridad y protección.
- H16. Utilizo diferentes métodos para mantener la fiabilidad y la privacidad.

Contenidos[1]:

1.1. Protección de los dispositivos digitales
1.2. Riesgos y amenazas en los entornos digitales
1.3. Protección de los contenidos digitales
1.4. Uso responsable de la tecnología

[1] Todos los contenidos están disponibles en el sitio del proyecto: https://www.beacyberpro.eu/

SESIÓN 1

Introducción. Conocimientos previos

- Diálogo inicial "Las ventajas y los riesgos que conocemos del uso del smartphone"
- Cuestionario para identificar hábitos de uso de dispositivos
- Lluvia de ideas acerca de un glosario de términos: noticias falsas, ransomware, phishing, spam, grooming, sexting, violación de derechos de autor, espionaje industrial, etc.

- Identificación de situaciones problemáticas en grupos cooperativos. ¿Qué tipo de problema es? ¿Cómo creéis que pueden resolverse?
- Resolución con toda la clase de las situaciones problemáticas:
- Accedes a la web del colegio/IES y sale un mensaje que solicita que instales una actualización de la app de comunicación con los docentes. Se trata de malware.
- Llevas hablando dos meses con una persona a través de Instagram, es muy agradable y te están planteando quedar en persona, pero cuando llegas al lugar de encuentro no parece ser quien decía.
- Te acaba de llegar un sms que pide que accedas a tu cuenta del colegio /IES e incluyas la clave, pero este mensaje no ha sido enviado desde el instituto.

SECCIÓN 2

Sextorsión[2]

- Actividad cooperativa "Lápices al centro". Recordamos lo trabajado en la sesión anterior.
- Se forman grupos de 4 personas y se plantean 4 preguntas o ejercicios acerca de lo trabajado en la sesión anterior.

Para iniciar el trabajo, todos los alumnos deben dejar los lápices/ordenadores en el centro de la mesa, esto significa que es tiempo para poder dialogar con los compañeros. En primer lugar, el responsable de la actividad número uno se encarga de leerla al resto de sus compañeros. Entre todos tiene que decidir cuál es la mejor forma para resolver la actividad a través del diálogo. Una vez han llegado a un acuerdo, todos los alumnos tienen que redactar de forma individual la solución a la que han llegado de forma grupal. Para ello, tienen que coger sus respectivos lápices/dispositivos, señal de que tienen que guardar silencio. Una vez han acabado todos de redactar las respuestas individualmente. Dejan de nuevo los lápices en el centro y el encargado de la segunda actividad la lee, repitiendo el mismo proceso que en la actividad anterior. Así, hasta acabar todos los ejercicios

- Visionado fragmento de serie Skam (caso sextorsión)
- Búsqueda de noticias en prensa sobre casos de sextorsión
- Completar el Árbol de decisión a partir de situación de posible *sexting*: "Si una persona desconocida está intentando ligar contigo en redes sociales…".

[2] Es posible que este tema no se considere adecuado para los planes de estudio de todos los centros. Te recomendamos que consultes con el consejo escolar o con un educador sexual antes de abordarlo

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

SESIÓN 3

Noticias falsas

- Diálogo inicial: ¿qué sabemos de las fake news? Compartimos algunas que conozcamos. Llevamos preparada alguna de actualidad
- Pautas para identificar una noticia falsa.
- Actividad cooperativa: “Los guardianes de la verdad”. Se facilitan varias noticias; deberán averiguar la verdad y la mentira que se entremezcla en cada una de ellas contrastando la información. Se puede seguir la dinámica de actividad cooperativa “Lápices al centro”.

MODULO 2. PROTEGER LOS DATOS PERSONALES Y LA PRIVACIDAD

OBJTIVOS DE APREDIZAJE

- Aplicar diferentes estrategias de prevención de riesgos físicos y psicológicos derivados del uso de las tecnologías digitales y guiar a otros (compañeros y alumnos) a aplicarlas.
- Ser capaz de diferenciar una gran variedad de efectos no deseados en el entorno derivados del uso de las tecnologías digitales y reflexiono sobre cómo minimizar este impacto.
- Guiar a otros (compañeros y alumnos) en el uso de recursos tecnológicos útiles para el desarrollo de la inclusión y/o el bienestar.

COMPETENCIAS BASADAS EN EL MARCO DIGCOMP

Gestión de la identidad digital

Habilidades:

- H1. Utilización crítica de diferentes identidades digitales, seleccionando la más adecuada en cada contexto o situación.
- H2. Selecciono y gestiono mi identidad digital en documentos y datos producidos por mí.
- H3. Utilizo diferentes formas de proteger mi identidad digital y verifico que funcionan correctamente.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

4.2. Protección de los datos personales y la privacidad en entornos digitales

Conocimientos:

- C1. Riesgos derivados de una incorrecta protección de datos o información personal.
- C2. Herramientas y métodos sencillos de protección de la información y los datos personales.
- C3. Aspectos y hechos básicos de las políticas de privacidad.
- C4 Herramientas y estrategias de protección de datos y contenidos personales (nivel intermedio
- C5 Recursos tecnológicos para la protección de datos.

Habilidades:

- H13. Utilizo y aplico diferentes métodos y herramientas para proteger mis datos, y soy capaz de ayudar a otros si es necesario.
- H14. Limito la información y los datos que comparto con otros; controlo la exposición pública de los datos y la información y ayudo a otros si es necesario.
- S15. Conozco las diferencias en las políticas de privacidad de los servicios que utilizo, y selecciono el servicio que mejor se adapta a mis intereses, asumiendo y controlando sus riesgos.
- S16. Ayudo a mis alumnos sobre cómo proteger su identidad digital y gestionar su huella digital.

Contenidos[4]:

- *Lección 2.1. La importancia de la protección de datos e información personal*
- *Lección 2.2. Herramientas y métodos para proteger la información y los datos personales en línea*
- *Lección 2.3. Herramientas y métodos para proteger la información y los datos personales fuera de línea*
- *Lección 2.4. Políticas de privacidad y juego limpio digital*

SESSION 1

Introducción. Conocimientos previos

- Diálogo inicial ¿sabemos qué datos no se pueden compartir? ¿cómo proteger nuestra información personal?
- Resolvemos en grupos cooperativos algunas situaciones problemáticas. Se puede seguir la dinámica de actividad cooperativa “Lápices al centro”.
  - Te hacen una foto cayéndote en plena calle y tus amigos quieren subirlo a tik tok
  - Una amiga ha publicado fotos del verano en la playa en Instagram y sales en bikini

[4] Todo el contenido puede encontrarse en la web del proyectoe: https://www.beacyberpro.eu/

- Una persona ha empezado a seguirte en Instagram y hace comentarios a tus fotos, dice que te conoce pero no sabes quién es

- Revisamos la política de privacidad de las redes sociales que usamos habitualmente todos juntos ¿Cómo lo tengo configurado? ¿cuál sería el modo más seguro? ¿qué supone?

SECCIÓN 2

Mis datos y yo

- Actividad cooperativa "Cabezas juntas numeradas" para recordar lo trabajado en la sesión anterior

  1. Se forman grupos de cuatro miembros y se numeran.
  2. El profesor lanza una pregunta y los alumnos pensarán de manera individual una respuesta. ¿Cómo evitar que tus amigos compartan información que no deseas compartir?
  3. Posteriormente se realiza una puesta en común en cada uno de los grupos "juntando las cabezas" a modo de corro. (De ahí el nombre de esta estrategia)
  4. Pasado unos minutos el profesor elige un número del 1 al 4 y el alumno correspondiente responderá la pregunta en nombre de su equipo.

- Presentamos algunas herramientas y métodos para proteger la información en línea y fuera de línea
- Completar el Árbol de decisión "Reflexiona sobre lo que publicas".

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

MODELO 3. PROTEGER LA SALUD, EL BIENESTAR Y EL MEDIO AMBIENTE

OBJETIVOS DE APRENDIZAJE

- Respetar los derechos de autor, las licencias y las restricciones de uso en los recursos que comparto y promover entre los alumnos el respeto a las normas de derechos de autor de los recursos digitales integrados en los entornos virtuales de aprendizaje.
- Tomar medidas para proteger los datos y la información sensible en los elementos compartidos digitalmente y animar a los estudiantes a hacer lo mismo con sus tareas.

COMPETENCIAS BASADAS EN EL MARCO DigComp

4.3.1. Uso ético y saludable de tecnologías digitales

Conocimientos:

- Conoce el efecto del uso prolongado de las tecnologías.
- Conoce los aspectos adictivos de las tecnologías.
- Comprende el impacto medioambiental de los ordenadores y dispositivos electrónicos y cómo puede hacer que duren más tiempo reciclando sus partes.
- Puede determinar si existen medios digitales adecuados y seguros que sean eficientes y rentables en comparación con otros medios.

Habilidades:

- H11. Puedo aplicar diferentes estrategias de prevención de riesgos físicos y psicológicos derivados del uso de las tecnologías digitales y guiar a otros para que las apliquen
- H12. Soy capaz de diferenciar una gran variedad de efectos no deseados en el entorno derivados del uso de las tecnologías digitales y reflexiono sobre cómo minimizar este impacto.
- H13. Guío a otros en el uso de recursos tecnológicos útiles para el desarrollo de la inclusión y/o el bienestar.

4.4. Proteger el medio ambiente

Habilidades:

- H14. Puedo mostrar diferentes formas de proteger el medio ambiente del impacto de las tecnologías digitales y su uso.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Contents[5]:

- *Lección 3.1. Efectos positivos y negativos del uso de ordenadores y tecnología digital*
- *Lección 3.2. Proteger la salud física durante el uso de la tecnología*
- *Lección 3.3. Proteger el bienestar psicológico en el entorno digital*
- *Lección 3.4. Tecnologías digitales para el bienestar social y la inclusión social*
- *Lección 3.5. Proteger el entorno*

[5] Todo el contenido puede encontrarse en la web del proyectoe: https://www.beacyberpro.eu/

SECCIÓN 1

- **Diálogo inicial:** Tecnología y salud. ¿El uso de dispositivos tecnológicos afecta a tu salud física? ¿y a la mental? Se identifican conocimientos previos y se aportan claves prácticas.

- Encuesta acerca de sus hábitos de uso de tecnología y salud

- Ejercicio de dramatización por equipos para reflejar conductas que favorecen o no la salud física y/o el bienestar psicológico usando tecnologías (mala ergonomía, mala iluminación, ignorar a alguien, etc).

- Actividad cooperativa “Folio giratorio” para resumir lo aprendido en la sesión

- El docente pide a los equipos una actividad (realizar un resumen, una redacción, un listado...). Para iniciarla, un alumno de cada equipo es el encargado de empezar a escribir una parte en un folio que ira rotando entre todos los compañeros. Cuando uno escribe, los demás deben de atender a lo que pone, deben ayudarle, aconsejarle y motivarle. Una vez ha hecho su aportación, pasa el folio al siguiente compañero y se repite la misma operación. Así, hasta que el folio haya pasado por todos los integrantes del equipo.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

MODULO 4. PERFILES PROFESIONALES

OBJETIVOS DE APRENDIZAJE

- Comunicar a los estudiantes una actitud positiva hacia las tecnologías digitales, haciéndolos conscientes de los posibles riesgos y límites, pero también generando confianza en que serán capaces de manejarlas para aprovechar los beneficios de las tecnologías y animándolos a utilizarlas de forma creativa y revisada.
- Desarrollar estrategias pedagógicas para prevenir, identificar y responder al uso inseguro de los dispositivos digitales y la publicación de contenidos digitales por parte de los estudiantes.
- Desarrollar estrategias para promover que los estudiantes protejan sus datos personales y su identidad digital en los entornos digitales.
- Desarrollar estrategias para prevenir, identificar y responder a los comportamientos de mis alumnos que afectan negativamente a su salud y bienestar utilizando las tecnologías digitales.

Contenidos[6]:

Lección 4.1. Perfiles Profesionales.

SECCIÓN 1

- **Diálogo inicial:** ¿Conoces a alguien que trabaje en ciberseguridad?
- Vídeo de experta en ciberseguridad explicando los distintos perfiles profesionales (Selva Orejón) y presentación del ebook de entrevistas a profesionales
- Diálogo acerca del vídeo y el libro presentados ¿Qué te ha sorprendido?
- Actividad individual "Si trabajara en ciberseguridad me gustaría hacer…" y "¿Qué le preguntaría a alguien que trabaje en ciberseguridad?".

SECCIÓN 2

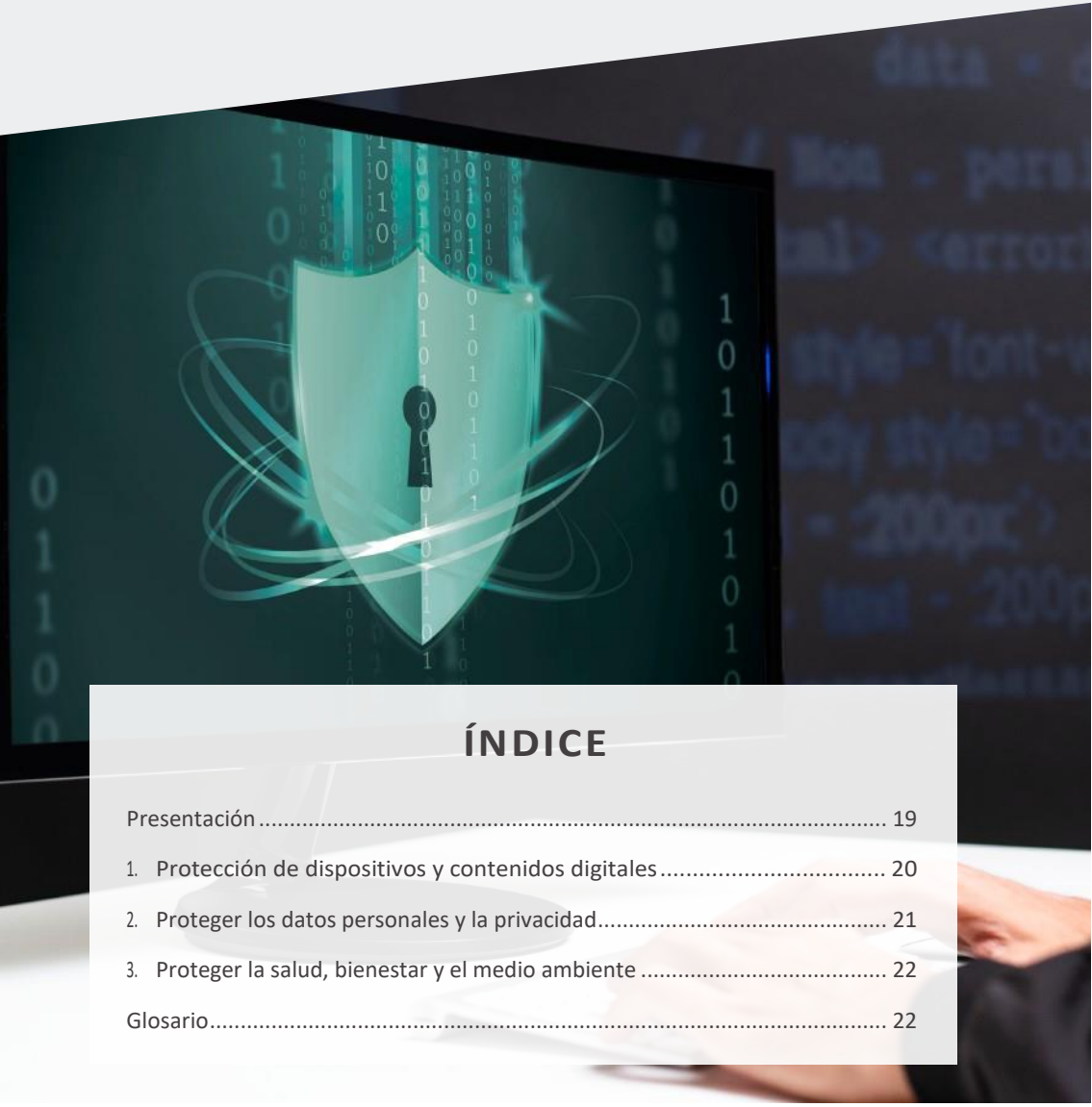
- Expertas en ciberseguridad visitantes (presencial u online de forma síncrona). Nos cuentan su experiencia
- Iniciamos debate a partir de las preguntas de la actividad individual de la sesión anterior y otras surgidas durante la presentación de las personas invitadas
- Generamos una presentación colaborativa en prezi para extraer las conclusiones de este módulo.

[5] Todo el contenido puede encontrarse en la web del proyectoe: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

CIBERSEGURIDAD PARA PADRES
Guía de buenas prácticas



ÍNDICE

Presentación 19

1. Protección de dispositivos y contenidos digitales 20
2. Proteger los datos personales y la privacidad 21
3. Proteger la salud, bienestar y el medio ambiente 22

Glosario 22

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

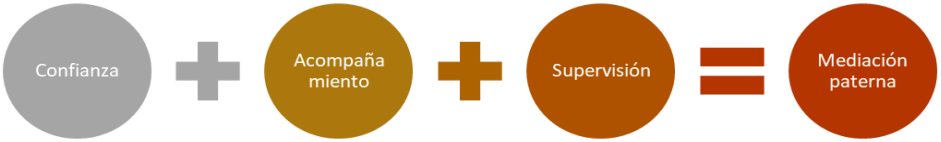
PRESENTACIÓN

Seguramente tu hijo/a tenga presencia en Internet y te preocupa que lo haga con seguridad. La finalidad de esta guía es generar comportamientos responsables e informados en tus hijos conforme a los principios básicos de la ciberseguridad.

Lo importante es que puedan y podáis juntos:

- Disfrutar de la Red
- Prevenir riesgos
- Detectar y afrontar problemas

Te daremos algunas claves esenciales para ejercer una mediación paterna y de ese modo garantizar la seguridad de tus hijos/as en la Red.



ALGUNAS CLAVES PRÁCTICAS ANTES DE EMPEZAR

- Mantén un diálogo abierto y sin juicios con tus hijos/as. Para ello formula preguntas abiertas que les permita compartir experiencias e inquietudes. No siempre será fácil ni estarán receptivos/as. Busca el momento para que la conversación pueda fluir
- Puedes utilizar algunos otros recursos para iniciar una conversación como:
    - Noticias de actualidad
    - Fragmentos de películas
    - Fragmentos de alguna serie que esté enfocada a público de su edad
- No lo hagas tú todo. Si crees que tu hijo/a puede tener algún problema habla con el tutor/a en el centro educativo para poder actuar de forma coordinada.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

1. Protección de dispositivos y contenidos digitales

Objetivos
• Generar una actitud positiva hacia las tecnologías digitales, generando conciencia de los posibles riesgos y límites, pero también generando confianza en que serán capaces de manejarlas para aprovechar los beneficios de las tecnologías y animándoles a utilizarlas de forma creativa y revisada. • Ser capaz de diferenciar una gran variedad de riesgos y amenazas en los entornos digitales: fake news, grooming, sexting, shareting, etc. (ver **glosario** al final de la guía) Y cómo actuar ante ellos. • Saber aplicar medidas de seguridad y protección y guiar a mis hijos/as para que las apliquen.

¿Qué puedes hacer?
CONFIANZA • Cuida tu reacción si te comentan que están teniendo un problema. No es momento de culpar sino de resolver juntos ACOMPAÑAMIENTO • Orienta a tus hijos/as en el uso adecuado de la tecnología. Podéis acordar algunas claves para un uso responsable o incluso firmar un pacto que quede visible en casa. • Sé un modelo a seguir • Compartir actividades en línea juntos. No es cuestión de invadir el espacio online y dar “me gusta” a todo lo que publican, pero si podéis pasar tiempo juntos en la Red buscando información SUPERVISIÓN • Mantente al día de su presencia en la red. Las apps que más usan, las redes sociales en que tienen perfil • Puedes hacer uso de recursos de control parental para limitar el acceso a sitios no seguros. (Qustodio, Secure Kids o Parental Click son algunos ejemplos) • Mantente atento/a por si reciben contenido inapropiado (que fomente comportamientos de riesgo o negativos o no comprensibles a su nivel de desarrollo)

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

2. Proteger los datos personales y la privacidad

Objetivos
• Aplicar diferentes estrategias de prevención de riesgos físicos y psicológicos derivados del uso de las tecnologías digitales y guiar a mis hijos/as a aplicarlas. • Ser capaz de diferenciar una gran variedad de efectos no deseados en el entorno derivados del uso de las tecnologías digitales y reflexiono sobre cómo minimizar este impacto. • Guiar en el uso de recursos tecnológicos útiles para el desarrollo de la inclusión y/o el bienestar.

¿Qué puedes hacer?
CONFIANZA • Genera un clima de confianza para que podáis hablar de vuestra presencia en la Red, de la información que recibís y la que compartís ACOMPAÑAMIENTO • Cread juntos contraseñas seguras para proteger los dispositivos • Revisad juntos las opciones de configuración de los dispositivos y servicios en la red para ser conscientes de la información que se comparte • Sé un modelo a seguir SUPERVISIÓN • Los códigos PEGI clasifican las Apps por edad, revisa las apps a las que tienen acceso para evitar el acceso a algunas inapropiadas • Si tienen un usuario limitado (ve a ajustes avanzados > usuarios o cuentas y sigue los pasos) restringe las aplicaciones o archivos a los que tienen acceso aplicando controles parentales si es preciso.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

3. Proteger la salud, el bienestar y el medio ambiente

Objetivos
• Desarrollar estrategias para prevenir, identificar y responder a los comportamientos de mis hijos/as que afectan negativamente a su salud y bienestar utilizando las tecnologías digitales.

¿Qué puedes hacer?
CONFIANZA • Habla abiertamente de los efectos nocivos del uso inadecuado de la tecnología en la salud, el bienestar o el medio ambiente para establecer acuerdos de uso correcto en casa y fuera de ella. Estos acuerdos deben dejar claros los horarios y lugares de conexión a la Red. Un uso excesivo puede afectar al sueño, las relaciones sociales o el estudio. • Confía en que cumplan estos acuerdos sin convertirte en un supervisor constante. ACOMPAÑAMIENTO • Sé un modelo a seguir. • Si tu hijo/a ha tenido un problema y hay otros menores implicados, contacta con sus padres o tutores para aclarar la situación y poder resolverla de forma coordinada SUPERVISIÓN • Observa el comportamiento de tu hijo y asegúrate de que se cumplen los acuerdos sobre el uso adecuado de la tecnología sin invadir su privacidad. • Establece normas y límites coherentes, consistentes y de forma consensuada con tus hijos/as acerca de tiempos y lugares para la conexión a la Red. El uso excesivo puede afectar al descanso, las relaciones sociales o el estudio.

Glosario

- Ciberacoso: Acoso a través de tecnologías digitales
- *Fake news*: Noticias falsas o bulos
- *Grooming*: Un adulto no es quien dice ser y se manipula al menor con fines económicos o sexuales
- *Sexting*: Un menor comparte contenidos con connotación sexual
- *Shareting*: la familia expone información privada de un menor

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

PROGRAMACIÓN DIDÁCTICA SOBRE
Videojuego Be@cyberpro

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

¿Qué es Be@CyberPro?

Be@CyberPro es un proyecto dedicado a reducir las diferencias de competencias y de género en la formación del sector de la ciberseguridad, inspirando a los estudiantes, capacitando a los profesores e implicando a los padres. Be@CyberPro es un juego de experiencia multilingüe inmersiva que se utiliza para explorar diversos perfiles y retos profesionales de la ciberseguridad. Se trata de un juego digital interactivo para navegador, de tal manera que puedan jugar a estudiantes de diversos contextos y con diferentes equipos.

Tiempo de juego: El juego -que incorpora todos los niveles- está diseñado para durar entre 40 minutos y 1 hora, la duración de una clase escolar normal.

Narrativa: Sigue el estilo de un juego de roles, en el que los jugadores asumen los papeles de personajes en un escenario ficticio. La protagonista principal, una chica que va al instituto, tiene que resolver una serie de retos relacionados con la ciberseguridad, asociados a diferentes perfiles profesionales de ciberseguridad, para ayudar a sus amigos y compañeros de clase.

Cómo jugar:

- Sigue el enlace para jugar al juego.
- Aparecerá el menú de inicio del juego con las siguientes opciones de botones: Nueva partida, Continuar y Opciones.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Cómo jugar:

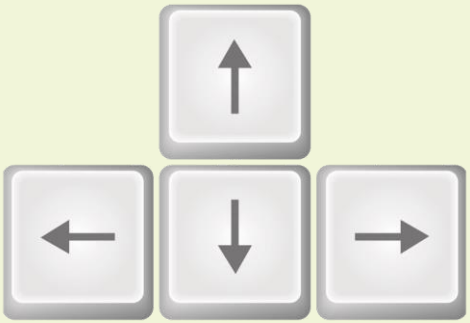
- Para empezar, haz clic en Nuevo juego con el ratón o trackpad.
- Cuando se cargue la pantalla, haz clic en cualquier lugar con el ratón o trackpad para iniciar las conversaciones entre los personajes.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Utiliza las flechas del teclado o haz clic en una zona para que el personaje se mueva.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union



- Acércate a los personajes del juego para entablar conversaciones.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

- Haz clic en cualquier lugar de la pantalla para continuar las conversaciones.
- Haz clic en los botones emergentes con el ratón o pulsa la tecla Intro para elegir tu respuesta.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

- Acércate a las puertas para pasar a otras habitaciones.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

- Pulsa Esc en cualquier momento para ver el menú de opciones.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

- Sigue las instrucciones de los personajes del juego para completar las tareas y aprender sobre ciberseguridad.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Enlace del juego: Se puede acceder en línea al juego desde todos los dispositivos en:
http://telprojectgames.com/CyberPro/Test/index.html

Apéndice: Guion gráfico de Be@CyberPro (en inglés):
https://drive.google.com/file/d/18HWpPqragp9Pstp7hgEsAmtg97Af2W8i/view?usp=sharing

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Antes de presentar el juego en el aula

A continuación, te ofrecemos algunas sugerencias sobre cómo podrías utilizar el juego en tu aula.

1. Juega tú mismo, familiarízate con los controles, la narrativa y el contenido didáctico del juego.

2. Considera la posibilidad de involucrar a los padres y tutores. Una posible forma de abrir la puerta a la participación de los padres o tutores sería enviar una carta a casa con los alumnos, o comunicar por otros medios tu plan de aprendizaje basado en el juego y sus beneficios a los padres y tutores. Hacerlo también podría ayudar a evitar confusiones si los alumnos llegan a casa y hablan de jugar en clase.

3. Dedica tiempo al juego constante en clase. Para asegurarte de que tus alumnos disfrutan de suficiente "tiempo de juego" con el videojuego Be@CyberPro para aprovechar sus beneficios, intenta:

- Incluir el tiempo de juego como una actividad designada en tu planificación didáctica.
- Utiliza el juego como principio o fin del aprendizaje. Al usarlo como punto de partida para el aprendizaje de la ciberseguridad, les permitirá a los alumnos sacar sus propias conclusiones sobre la importancia de la ciberseguridad antes de que el experto explique el concepto en detalle y lo refuerce.
- Crea una serie de estaciones de aprendizaje, uno de los cuales será el juego.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Cómo presentarles a los estudiantes las estaciones de aprendizaje

Las estaciones de aprendizaje son lugares físicos en el aula donde se pide a los alumnos que resuelvan un problema y respondan a algunas preguntas utilizando los materiales proporcionados. Pueden servir para que los alumnos jueguen individualmente, en parejas o en pequeños grupos durante la clase.

- Dedica tiempo a presentar de forma muy explícita las nuevas estaciones de aprendizaje a la clase y a discutir las reglas asociadas al uso de las estaciones de aprendizaje.

- Antes de empezar, explica claramente el comportamiento que se espera de los alumnos al utilizar las estaciones de aprendizaje y las consecuencias de no cumplir estas expectativas. A continuación, presenta la nueva estación de aprendizaje a tus alumnos mediante un ejemplo de los siguientes pasos.

- Si procede, utiliza un temporizador que los alumnos vean y oigan para controlar el tiempo que pasan en las estaciones de aprendizaje.

- Enseña a los alumnos cómo vas a llamar su atención mientras están en la estación de aprendizaje (por ejemplo, levantando la mano).

- Explica detalladamente el propósito de la actividad seleccionada en la que van a trabajar. "Esto es lo que vais a aprender en esta estación de aprendizaje".

- Enseña solo lo imprescindible para que los alumnos entiendan y se sientan cómodos trabajando en las actividades. Demuestra cómo limpiar el área y cambia al siguiente estudiante cuando se apague el temporizador.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Cómo utilizar el videojuego en tu clase

1. Presenta el tema brevemente y explica a los alumnos los objetivos y la narrativa del juego antes de jugar.
2. Establece una base rápida de conocimientos antes del juego. Pregunta, levantando la mano o de forma similar, si alguien sabe algo sobre ciberseguridad o si ha tenido alguna vez un problema de ciberseguridad.
3. Deja que los alumnos jueguen al primer nivel y pídeles que pausen el juego cuando hayan terminado.
4. Una vez que todos hayan terminado el primer nivel, organiza una sesión informativa y comenta con ellos lo que han aprendido hasta ahora. Algunos puntos de debate recomendados son:
    - Lo que los alumnos han aprendido de este Nivel.
    - Lo que piensan sobre lo que han aprendido hasta ahora.
    - Si alguien ha tenido alguna experiencia similar.
    - Si alguien ha tenido alguna dificultad para entender el material.
    - Si los alumnos están motivados para continuar con el juego.
5. Pide a los alumnos que continúen con el juego siguiendo esta misma estructura (nivel de juego, y luego puntos de discusión)
6. Cuando los estudiantes hayan completado el juego, distribúyeles la herramienta de evaluación del juego (es decir, el cuestionario en línea).
7. Utiliza los datos recogidos de las charlas y los comentarios para crear lecciones a partir de tus conclusiones. Por ejemplo, céntrate en un punto conflictivo común.

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Apoyo al aprendizaje

El uso del aprendizaje basado en juegos, que incorpora objetivos, reglas, retos e interacciones, puede ayudar a involucrar a los estudiantes y aumentar los resultados del aprendizaje. El aprendizaje basado en juegos también puede:

- Construir una conexión emocional con el aprendizaje y la materia.
- Proporcionar una oportunidad para la retroalimentación y la práctica.
- Adaptarse a la enseñanza individualizada.

Como parte del uso educativo de la tecnología de la información y la comunicación, los juegos digitales pueden utilizarse como herramientas de aprendizaje, motivadores y generadores de curiosidad. Así pues, actualmente se los considera como un medio eficaz para optimizar el aprendizaje y el rendimiento de los estudiantes en la práctica educativa diaria. La relación positiva entre el compromiso de los estudiantes y su recepción de información mientras usan juegos digitales se ha confirmado en varios estudios independientes en los últimos años (Cojocariua, Boghiana, 2014; Papadakis, 2018).

Project number: 2018-1-ES01-KA201-050461
Co-funded by the Erasmus+ Programme of the European Union

Enlace online al juego

Puedes acceder virtualmente al juego desde cualquier dispositivo en:
http://telprojectgames.com/CyberPro/Test/index.html

Página del proyecto

https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

REFERENCIAS

Ahuja, M. K. (2002). Women in the information technology profession: A literature review, synthesis and research agenda. *European Journal of Information Systems*, *11*(1), 20-34.

Armstrong, D. J., Riemenschneider, C. K., Allen, M. W., & Reid, M. F. (2007). Advancement, voluntary turnover and women in IT: A cognitive study of work–family conflict. *Information & Management*, *44*(2), 142-153.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, *12*(1), 24-31.

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight profi-ciency levels and examples of use*, EUR 28558 EN, doi:10.2760/38842

Cojocariu, V. M., & Boghian, I. (2014). Teaching the relevance of game-based learning to preschool and primary teachers. *Procedia-Social and Behavioral Sciences*, *142*, 640-646.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

Carretero, S., Vuorikari, R., & Punie, Y. (2016*). DigComp: Marco Europeo de Competencias Digitales para la ciudadanía*.

ENISA (The European Union Agency for Cybersecurity) (2020). *ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Erixon, F., & Lamprecht, P. (2018). The next steps for the digital single market: From where do we start. *ECIPE Policy Brief*, *2*, 2018.

Heaton, C. A. N., & McWhinney, G. (1999). Women in management: the case of MBA graduates. *Women in Management Review*.

Kohler, K. (2020). Estonia's National Cybersecurity & Cyberdefense Posture.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2).

Papadakis, S. (2018). Evaluating pre-service teachers' acceptance of mobile devices with regards to their age and gender: a case study in Greece. *International Journal of Mobile Learning and Organisation*, *12*(4), 336-352.

Parasuraman, S., Purohit, Y. S., Godshalk, V. M., & Beutell, N. J. (1996). Work and family variables, entrepreneurial career success, and psychological well-being. *Journal of vocational behavior*, *48*(3), 275-300.

Poster, W. R. (2018). Cybersecurity needs women.

Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, (2018/06).

Reischuk, R. (2019). *Let's Encrypt: Cybersecurity disruptieren*.

Sobers, R. (2019). must-know cybersecurity statistics for 2019. *Varonis.*

Stellini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Security & Privacy*, *18*(1), 46-54.

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National Cyber Security Strategies: Management, Unification and Assessment.

Trauth, E. M., Quesenberry, J. L., & Morgan, A. J. (2004, April). Understanding the under representation of women in IT: Toward a theory of individual differences. In *Proceedings of the 2004 SIGMIS conference on Computer personnel research: Careers, culture, and ethics in a networked environment* (pp. 114-119). Ventures, 2017

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

SOCIOS

Universidad Europea de Madrid (Spain)

- Eva Jiménez García
- Gonzalo Mariscal Vivas
- Javier Fernández Collantes
- Luis Antonio López Fraile
- Sara Esteban Gonzalo
- Sonia Martínez Requejo

Colegio JOYFE (Spain)

Munster Technological University (Ireland)

European Software Institute – Center Eastern Europe (Bulgaria)

- Christina Todorova
- Pavel Varbanov

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

SOCIOS

The Irish Computer Society
(Ireland)

- Liz Mc Carthy

PROMPT-H LTD
(Hungary)

- Annamaria Kacsur

SZÁMALK-Szalézi Vocational and Technical School
(Hungary)

- Ildikó dr Sediviné Balassa
- Gabriella Kőhegyi

University of Alcala
(Spain)

- Maite Villalba Benito
- Luis Fernández Sanz
- Ana Castillo
- Inés López Baldominos
- Vera Pospelova

125th High School «Boyan Penev»
(Bulgaria)

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

© Be@CyberPro, 2021 ERASMUS+ Project 2018-1-ES01-KA201-050461

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The contents of this report may be downloaded, reproduced, distributed and printed for private study purposes, research and teaching, or for use in non-commercial products or services, provided that authors are adequately recognized as the source and holders of intellectual property rights, without implying in any way that they approve the resulting views, products or services. For those contents in which specifically it is indicated that they come from third parties, any request must be addressed to the original source to manage proper permissions.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union